

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский авиационный институт
(национальный исследовательский университет)»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ Козорез Д.А.
“26” июня 2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (000134382)

Методы и средства защиты компьютерной информации

(указывается наименование дисциплины по учебному плану)

Направление подготовки 09.03.01 Информатика и вычислительная техника

Квалификации выпускника Бакалавр

Профиль подготовки Автоматизированные системы обработки информации и управления

Форма обучения очная
(очно, очно-заочное, заочное)

Выпускающая кафедра МСиИТ

Обеспечивающая кафедра МСиИТ

Кафедра-разработчик рабочей программы МСиИТ

Семестр	З.Е.	Трудоемкость, час.	Лекций, час.	Практич. занятий, час.	Лаборат. работ, час.	СРС, час.	Экзаменов, час.	Форма промежуточ- ного контроля
8	4	144	32	0	32	44	36	Э
Итого	4	144	32	0	32	44	36	

Москва
2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Разделы рабочей программы

1. Цели освоения дисциплины. Перечень планируемых результатов обучения.
2. Место дисциплины в структуре образовательной программы.
3. Структура и содержание дисциплины.
4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.
5. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.
6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.
8. Методические указания для обучающихся по освоению дисциплины.
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.
10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Приложения к рабочей программе дисциплины

Приложение 1. Аннотация рабочей программы

Приложение 2. Прикрепленные файлы

Программа составлена в соответствии с требованиями СУОС МАИ, разработанного на основе модифицированных ФГОС ВО (3++) по направлению 09.03.01 Информатика и вычислительная техника

Авторы программы:

Уханова А.М.

Заведующий обеспечивающей кафедрой

МСиИТ

Программа одобрена:

Заведующий выпускающей кафедрой

МСиИТ

Директор выпускающего филиала

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ КОМПЕТЕНЦИЙ И РЕЗУЛЬТАТОВ ОБУЧЕНИЯ.

Целью освоения дисциплины Методы и средства защиты компьютерной информации является достижение следующих результатов освоения(РО):

N	Шифр	Результат обучения

Перечисленные РО являются этапом формирования следующих компетенций:

N	Шифр	Компетенция

Индикаторы достижения компетенций, служащие для проверки сформированности части соответствующей компетенции:

N	Шифр	Индикатор компетенций

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.

Дисциплина Методы и средства защиты компьютерной информации является предшествующей и последующей для следующих дисциплин:

N	Предшествующие дисциплины	Последующие дисциплины

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы), 144 часа(ов).

Модуль	Раздел	Лекции	Практич. занятия	Лаборат. работы	СРС	Всего часов	Всего с экзаменами и курсовыми
Методы и средства защиты компьютерной информации (8 семестр).	Основные понятия и определения курса. Классификация угроз информационной безопасности.	2	0	0	4	6	144
	Федеральные законы РФ в области защиты информации, стандарты ИБ.	2	0	0	4	6	
	Руководящие документы ФСТЭК России.	2	0	0	0	2	
	Аутентификация, идентификация, авторизация.	2	0	0	0	2	
	Протоколы сетевой аутентификации.	4	0	8	8	20	

	Основы криптографии, инфраструктура открытых ключей.	4	0	4	4	12	
	Вредоносное программное обеспечение.	4	0	4	6	14	
	Межсетевые экраны.	4	0	8	6	18	
	Классификации уязвимостей. Системы обнаружения вторжений IDS/IPS.	4	0	4	6	14	
	DLP-системы, DMZ, DPI, аудит ИБ, тестирование на проникновение, WAF.	4	0	4	6	14	
Всего		32	0	32	44	108	144

3.1.Лекции

№ п/п	Раздел дисциплины	Объем, часов	Тема лекции
1	1.1.Основные понятия и определения курса. Классификация угроз информационной безопасности.	2	Основные понятия и определения курса. Классификация угроз информационной безопасности.
2	1.2.Федеральные законы РФ в области защиты информации, стандарты ИБ.	2	Федеральные законы РФ в области защиты информации, стандарты ИБ.
3	1.3.Руководящие документы ФСТЭК России.	2	Руководящие документы ФСТЭК России.
4	1.4.Аутентификация, идентификация, авторизация.	2	Аутентификация, идентификация, авторизация.
5	1.5.Протоколы сетевой аутентификации.	4	Протоколы сетевой аутентификации.
6	1.6.Основы криптографии, инфраструктура открытых ключей.	4	Основы криптографии, инфраструктура открытых ключей.
7	1.7.Вредоносное программное обеспечение.	4	Вредоносное программное обеспечение.
8	1.8.Межсетевые экраны.	4	Межсетевые экраны.
9	1.9.Классификации уязвимостей. Системы обнаружения	4	Классификации уязвимостей. Системы обнаружения вторжений IDS/IPS.

	вторжений IDS/IPS.		
10	1.10.DLP-системы, DMZ, DPI, аудит ИБ, тестирование на проникновение, WAF.	4	DLP-системы, DMZ, DPI, аудит ИБ, тестирование на проникновение, WAF.
Итого:		32	

3.2.Содержание лекций.

1.1.1. Основные понятия и определения курса. Классификация угроз информационной безопасности. (АЗ: 2, СРС: 4)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: Определения «Информационная безо-пасность», «конфиденциальность», «целостность», «доступность информа-ции», «угроза», «автоматизированная система», виды защиты информации, цели защиты информации, понятия «угроза ИБ», «модель угроз», классификация угроз информационной безопасности.

1.2.1. Федеральные законы РФ в области защиты информации, стандарты ИБ. (АЗ: 2, СРС: 4)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: Краткий обзор ФЗ-149 «Об информа-ции, информатизации и защите информации», ФЗ-152 «О персональных данных», ФЗ-98 «О коммерческой тайне», ФЗ-63 «Об электронной подписи», понятие «стандарт», стандарт Министерства обороны США «Крите-рии оценки доверенных компьютерных систем», ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности инфор-мационных технологий», обзор «Мето-дологии управления информационными технологиями» – COBIT 5, Междуна-родные стандарты менеджмента инфор-мационной безопасности серии ISO 27000, стандарты организации NIST в области ИБ, цели, задачи и структура стандарта Банка России СТО БР ИББС, Стандарт PCI DSS.

1.3.1. Руководящие документы ФСТЭК России. (АЗ: 2, СРС: 0)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: Назначение ФСТЭК России, функции ФСТЭК России, обзор Руководящих документов «Классификация по уровню контроля отсутствия недеklarирован-ных возможностей», «Классификация автоматизированных систем и требования по защите информации», «Межсетевые экраны. Показатели защищенности от несанкционированно-го доступа к информации», «СВТ. Показатели защищенности от НСД к информации», классификация систем обнаружения вторжений, обзор требований постановления правительст-ва РФ № 1119 от 01.11.2012 года «Об

утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.4.1. Аутентификация, идентификация, авторизация. (АЗ: 2, СРС: 0)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: Понятия «аутентификация», «идентификация», «авторизация», классификация средств идентификации и аутентификации с точки зрения применяемых технологий, электронные ключи Touch Memory, технология RFID, классификация RFID-меток, карты с магнитной полосой, штрих-коды, биометрия, статические и динамические методы биометрической аутентификации, парольная аутентификация, одноразовые пароли, варианты реализации систем аутентификации по одноразовым паролям, двухфакторная аутентификация, смарт-карты, классификация смарт-карт по способу обмена со считывающим устройством, области применения смарт-карт, рутокен, eToken.

1.5.1. Протоколы сетевой аутентификации. (АЗ: 4, СРС: 0)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: Протокол аутентификации Kerberos, понятия ticket, Key Distribution Center, протоколы аутентификации для удалённого доступа, протокол аутентификации RADIUS, понятия клиент RADIUS, сервер RADIUS, посредник RADIUS, служба проверки подлинности в интернете IAS.

1.6.1. Основы криптографии, инфраструктура открытых ключей. (АЗ: 4, СРС: 0)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: Понятие криптографии, принцип симметричного шифрования, шифрования с открытым ключом, понятие «ключ» в криптографии, цифровая подпись, работа односторонней хэш-функции, цифровые сертификаты ключей, цель ЭЦП на сертификате, распространение сертификатов, серверы-депозитарии, основы инфраструктуры открытых ключей, понятия «центр сертификации», «список отозванных ключей», различные модели PKI, аутентификация с использованием сертификатов открытого ключа.

1.7.1. Вредоносное программное обеспечение. (АЗ: 4, СРС: 2)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: Понятия «антивирусная программа», «вредоносное ПО», «компьютерный вирус», признаки возможного заражения компьютера, обзор вирусной активности за текущий год, категории угроз, рекламные программы, backdoor-программы, фишинг, программы-шутки, обманные программы, bot-сети, эксплойты, фарминг.

1.8.1. Межсетевые экраны. (АЗ: 4, CPC: 2)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: Понятие «Межсетевой экран», функции межсетевых экранов, способы реализации МЭ, фильтр пакетов, принципы обработки пакетов данных в МЭ, типы МЭ согласно уровням модели OSI, управляемые коммутаторы, сетевые фильтры, статическая фильтрация в сетевых фильтрах, шлюзы сеансового уровня, фильтры контроля состояния канала связи, принцип работы фильтра с многоступенчатым порядком установления соединений, шлюзы, транслирующие адреса или сетевые протоколы, режимы работы шлюзов NAT, посредники прикладного уровня, типы посредников прикладного уровня, инспекторы состояния, другие возможности МЭ.

1.9.1. Классификации уязвимостей. Системы обнаружения вторжений IDS/IPS. (АЗ: 4, CPC: 2)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: Понятия «уязвимость», «дефект безопасности», типы классификаций уязвимостей, различные классификации и реестры уязвимостей, классификация вредоносного ПО, классификация уязвимостей программных систем, NVD, CVE, CPE, OSVDB, бюллетени по безопасности Microsoft, бюллетени по безопасности Adobe, реестры уязвимостей ОС debian, ubuntu, redhat linux, OWASP, русскоязычный репозиторий языка OVAL, банк данных угроз безопасности информации ФСТЭК России, системы обнаружения вторжений (атак), цель обнаружения атак, признаки атак, классификация COA по принципу реализации, распределённые COA (distributed IDS), компоненты dIDS, системы предотвращения вторжений (IPS), системы Security Information and Event Management (SIEM), задачи систем SIEM, возможности систем SIEM, источники данных для систем SIEM.

1.10.1. DLP-системы, DMZ, DPI, аудит ИБ, тестирование на проникновение, WAF. (АЗ: 4, CPC: 2)

Тип лекции: Информационная лекция

Форма организации: Лекция

Описание: назначение DLP-систем, структура DLP-систем, классификация DLP-систем по способу обнаружения утечки данных, перечень контролируемых действий, демилитаризованная зона (DMZ), конфигурация с одним МЭ конфигурация с двумя МЭ, технология DPI (Deep Packet Inspection), аудит ИБ, виды аудита ИБ, тестирование на проникновение, объекты тестирования,

этапы аудита ИБ, перечень ПО для оценки основных функций безопасности сети, технология WAF (Web Application Firewall), основные режимы развертывания WAF, модели безопасности WAF, основные возможности WAF.

3.3. Практические занятия

Не предусмотрено учебным планом.

3.4. Содержание практических занятий

3.5. Лабораторные работы

№ п/п	Раздел дисциплины	Наименование лабораторной работы	Объем, часов
1	1.5.Протоколы сетевой аутентификации.	Моделирование локальных компьютерных сетей с использованием среды CISCO Packet Tracer (часть 1).	4
2	1.5.Протоколы сетевой аутентификации.	Моделирование локальных компьютерных сетей с использованием среды CISCO Packet Tracer (часть 2).	4
3	1.6.Основы криптографии, инфраструктура открытых ключей.	Удаление информации, затирание свободного места, очистка реестра, создание зашифрованных контейнеров.	4
4	1.7.Вредоносное программное обеспечение.	Применение различных типов антивирусных программ и утилит для борьбы с вредоносным программным обеспечением.	4
5	1.8.Межсетевые экраны.	Изучение принципов установки и настройки межсетевых экранов на примере Comodo free firewall, контроль сетевых подключений (TCPview, netstat).	4
6	1.8.Межсетевые экраны.	Изучение принципов установки и настройки межсетевых экранов на примере Comodo free firewall, контроль сетевых подключений (TCPview, netstat).	4
7	1.9.Классификации уязвимостей. Системы обнаружения вторжений IDS/IPS.	Анализ уязвимостей операционных систем с помощью Nessus, эксплуатация критических уязвимостей с помощью набора эксплоитов metasploit framework.	4
8	1.10.DLP-системы, DMZ, DPI, аудит ИБ, тестирование на проникновение, WAF.	Работа с программой исследования и аудита безопасности сети nmap, анализатором сетевого трафика Wireshark.	4

Итого:	32
--------	----

3.6.Содержание лабораторных работ

1.5.1. Моделирование локальных компьютерных сетей с использованием среды CISCO Packet Tracer (часть 1). (А3: 4, CPC: 4)

Форма организации: Лабораторная работа

1.5.2. Моделирование локальных компьютерных сетей с использованием среды CISCO Packet Tracer (часть 2). (А3: 4, CPC: 4)

Форма организации: Лабораторная работа

1.6.1. Удаление информации, затирание свободного места, очистка реестра, создание зашифрованных контейнеров. (А3: 4, CPC: 4)

Форма организации: Лабораторная работа

1.7.1. Применение различных типов антивирусных программ и утилит для борьбы с вредоносным программным обеспечением. (А3: 4, CPC: 4)

Форма организации: Лабораторная работа

1.8.1. Изучение принципов установки и настройки межсетевых экранов на примере Comodo free firewall, контроль сетевых подключений (TCPview, netstat). (А3: 4, CPC: 2)

Форма организации: Лабораторная работа

1.8.2. Изучение принципов установки и настройки межсетевых экранов на примере Comodo free firewall, контроль сетевых подключений (TCPview, netstat). (А3: 4, CPC: 2)

Форма организации: Лабораторная работа

1.9.1. Анализ уязвимостей операционных систем с помощью Nessus, эксплуатация критических уязвимостей с помощью набора эксплоитов metasploit framework. (А3: 4, CPC: 4)

Форма организации: Лабораторная работа

1.10.1. Работа с программой исследования и аудита безопасности сети nmap, анализатором сетевого трафика Wireshark. (А3: 4, CPC: 4)

Форма организации: Лабораторная работа

3.7.Курсовые работы и проекты по дисциплине

3.8.Промежуточная аттестация

1.

Прикрепленные файлы: Примеры вопросов.docx

4. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Основная и дополнительная литература по дисциплине
2. Ресурсы информационно-телекоммуникационной сети «Интернет».
3. Ресурсы научно-технической библиотеки МАИ.
4. Информационные стенды кафедры.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Описание показателей, критерии оценивания компетенций и описание шкал оценивания осуществляются в соответствии с Положением о балльно-рейтинговой системе оценки результатов обучения студентов по дисциплине (Приказ №42 от 04.04.2014 «Об утверждении положения «Рейтинг по дисциплине»).

Для оценивания интегрированных и практико-ориентированных заданий обучающихся используются следующие критерии по 100-балльной шкале:

1. Формулирование представленной информации в виде проблемы;
2. Предложение способа решения проблемы;
3. Обоснование способа решения проблемы;
4. Демонстрация способа решения проблемы.

Оценивание осуществляется по следующей шкале:

100-балльная шкала	Результат освоения
менее 40	Критерий не сформирован
41-70	Критерий четко не выражен
71-100	Критерий выражен четко

Для оценивания ситуационных заданий используется следующая шкала:

100-балльная шкала	Результат освоения
менее 30	обучающийся не может сформулировать проблему, представленную в задании
31-50	обучающийся формулирует поставленную задачу, у него сформированы изолированные знания и умения, однако

	отсутствуют интегрированные понятия и навыки, в результате чего допущены ошибки в решении и задание не выполнено
51-80	задание выполнено, обучающийся применяет знания для решения поставленной проблемы, однако не сформированы компетенции, вследствие чего обучающийся испытывает затруднения в демонстрации способов решения задачи
81-100	задание выполнено как в теоретическом, так и в практическом плане, обучающийся легко демонстрирует свою компетентность по данному вопросу

Фонды оценочных средств, позволяющие оценить результаты обучения, включают в себя:

- вопросы к промежуточной аттестации.

Перечень компетенций и этапы их формирования приведены в следующей таблице:

N	Шифр	Компетенция	Этапы формирования компетенции

Вопросы к промежуточной аттестации

«Методы и средства защиты компьютерной информации»

1. Экзамен (8 семестр)

Прикрепленные файлы: Примеры вопросов.docx

6. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

а) основная литература:

1. Шаньгин В. Ф., Информационная безопасность компьютерных систем и сетей [Электронный ресурс] : Учебное пособие / В.Ф. Шаньгин. М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. Режим доступа: <http://znanium.com/bookread.php?book=423927>
2. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. Режим доступа: <http://znanium.com/bookread.php?book=405000>

б) дополнительная литература:

1. Жукова М.Н., Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : Учебное пособие / М.Н. Жукова, В.Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. Режим доступа: <http://znanium.com/bookread.php?book=463061>
2. Кузнецов, И. Н. Бизнес-безопасность [Электронный ресурс] : Практическое руководство / И. Н. Кузнецов. - 3-е изд. - М.: Дашков и К, 2013. - 416 с. Режим доступа: <http://znanium.com/bookread.php?book=430343>

7. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Для обеспечения образовательного процесса по дисциплине обучающимся предоставляется возможность круглосуточного дистанционного индивидуального доступа к электронным библиотечным системам из любой точки, в которой имеется доступ к сети «Интернет».

Наименование ресурса	Интернет-ссылка на ресурс
"ZNANIUM.COM"	
Электронная библиотечная система "ZNANIUM.COM".	http://znanium.com
ООО "Издательство Лань"	
Электронная библиотечная система ООО "Издательство Лань".	e.lanbook.com
ООО "Электронное издательство ЮРАЙТ"	
Электронная библиотечная система ЮРАЙТ. ЭБС "Легендарные книги"	http://biblio-online.ru , https://biblio-online.ru/catalog/legendary
Электронная библиотека МАИ	
Электронная библиотека МАИ (собственность МАИ).	http://elibrary.mai.ru/MegaPro2/Web
Электронная библиотека Консорциума аэрокосмических вузов России	
Электронная библиотека Консорциума аэрокосмических вузов России.	http://elsau.ru
Библиотека РФФИ	
Библиотека РФФИ	http://www.rfbr.ru/rffi/ru/library
Единое окно доступа к образовательным ресурсам	
Единое окно доступа к образовательным ресурсам	http://window.edu.ru/
Polpred.com	
Polpred.com. Обзор СМИ	http://polpred.com
ООО "РУНЭБ"	
Электронная библиотечная система eLIBRARY.	http://elibrary.ru

ООО "Национальный цифровой ресурс "Рукоонт"	
ООО "Национальный цифровой ресурс "Рукоонт".	http://text.rucont.ru
ООО "ИВИС"	
ООО "ИВИС".	http://ivis.ru
ООО "Интегратор авторского права"	
ООО "Интегратор авторского права" IQlib.	http://www.iqlib.ru/
ФГБУ "РГБ"	
Электронная библиотека диссертаций РГБ.	http://dvs.rsl.ru
Национальная электронная библиотека (НЭБ).	http://нэб.рф
НП НЭИКОН	
Некоммерческое партнерство "Национальный Электронно-Информационный Консорциум".	http://archive.neicon.ru
Научные полнотекстовые ресурсы издательства Springer (архив).	http://link.springer.com/
Научные полнотекстовые журналы издательства Taylor&Francis Group (архив).	http://www.tandfonline.com/
База данных GreenFile компании EBSCO.	http://www.greeninfoonline.com.
Внешнеэкономическое объединение "Академинторг"	
American Physical Society American Mathematical Society	http://publish.aps.org/ http://www.ams.org/mathscinet/index.html
ФГБУ "ГПНТБ России"	
База данных Web of Science (правообладатель - Thomson Reuters, с 03.10.2016 г. - Clarivate Analytics).	www.webofscience.com
База данных Scopus издательства Elsevier.	http://scopus.com
Springer Customer Service Center GmbH в научных и образовательных целях. Springer Nature	http://link.springer.com/ http://www.nature.com/
База данных компании EBSCO Publishing: БД CASC. БД MathSciNet via EBSCOhost .	http://search.ebscohost.com
Научные полнотекстовые журналы и книги издательства Elsevier.	http://www.sciencedirect.com http://www.elsevierscience.ru/products/science-direct
РФФИ	
Научные полнотекстовые англоязычные журналы American Chemical Society.	http://pubs.acs.org .

8.МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Эффективным способом развития творческих способностей студентов при изучении дисциплины является самостоятельная работа, которая нацелена на проработку студентами материала прошедших контактных занятий и подготовку к предстоящим занятиям.

Самостоятельная работа студентов проводится ими в соответствии с собственными возможностями. Можно, однако, рекомендовать групповое изучение материалов, обеспечивающее совместную работу нескольких студентов, что положительно влияет на качество проработки программы курса.

В то же время высокая степень усвоения изучаемой дисциплины достигается при постоянной работе студентов над текущим материалом. В этой связи желательна проработка лекционного материала в день его прочтения, что позволяет, во-первых, оперативно (на следующей лекции) снимать возникающие вопросы и, во-вторых, создавать багаж знаний по дисциплине задолго до промежуточной аттестации.

При подготовке к практическим занятиям также необходима проработка лекционного материала. Это позволит осознанно работать с предлагаемым материалом преподавателем на практическом занятии, а, следовательно, закладывать базу методик и приемов при решении практических задач.

При изучении материала необходимо делать акцент не на зазубривании материала, а на понимании его физической сути, что развивает мышление и позволяет понять методологию изучаемой дисциплины.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Дисциплина ориентирована на применение компьютерной техники, ресурсов информационно-телекоммуникационной сети «Интернет», электронной библиотеки МАИ для поиска, сбора, хранения, обработки и представления информации.

Программное обеспечение, Интернет-ресурсы, электронные библиотечные системы:

Программное обеспечение:

- ОС Microsoft Windows 7 Prof.;
- Microsoft Word;
- ОС Kali Linux;
- TrueCrypt;
- Piriform Recuva;
- Kaspersky Virus Removal Tool, DrWeb CureIt;
- Comodo free firewall;

Интернет-ресурсы:

- <http://securitylab.ru>
- <http://data-sec.ru>
- <http://fstec.ru/>
- <http://www.anti-malware.ru/>
- <http://msdn.microsoft.com>

10. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Лекционные занятия

1.1. Комплект электронных презентаций/слайдов.

1.2. Аудитория, оснащенная презентационной техникой (проектор, экран, компьютер)

2. Лабораторные работы

2.1. Аудитория, оснащенная презентационной техникой (проектор, экран, компьютер).

2.2. Персональные компьютеры – 27 рабочих мест.

2.3. Локальная вычислительная сеть с доступом в Интернет.

3. Практические занятия

3.1. Компьютерный класс.

3.2. Презентационная техника (проектор, экран, компьютер).

3.3. Пакеты ПО общего назначения (Текстовый редактор – Microsoft Word),

3.4. Специализированное ПО: ПО для шифрования на лету TrueCrypt, антивирусные утилиты Kaspersky Virus Removal Tool, DrWeb CureIt, межсетевой экран Comodo free firewall, операционная система для проведения аудита безопасности Kali Linux.

Аннотация рабочей программы

Дисциплина Методы и средства защиты компьютерной информации является частью Блока 1 Дисциплины дисциплин подготовки студентов по направлению подготовки 09.03.01 Информатика и вычислительная техника. Дисциплина реализуется на Ступино факультете «Московский авиационного института (национального исследовательского университета)» кафедрой (кафедрами) МСиИТ.

Дисциплина нацелена на формирование следующих компетенций: .

Содержание дисциплины охватывает круг вопросов, связанных с: -освоением понятий информационная безопасность, конфиденциальность, целостность, доступность информации, угроза, автоматизированная система, несанкционированный доступ, администратор безопасности, политика безопасности, режим разграничения доступа, межсетевые экраны, системы обнаружения вторжений, классификации уязвимостей программного обеспечения, аутентификация, идентификация, авторизация;

- изучением основных принципов обеспечения информационной безопасности, типов межсетевых экранов, классификаций угроз информации, группы персональных данных, категории вредоносного программного обеспечения, назначение и основные функции DLP-систем;

- применением сканеров уязвимостей для обнаружения текущих уязвимостей в информационных системах, получение навыков моделирования локальных компьютерных сетей с использованием среды CISCO Packet Tracer;

- получением навыков работы с nmap – инструментом исследования и аудита безопасности сети, являющимся также сканером портов;

- освоением различных типов антивирусных программ и утилит для борьбы с вредоносным программным обеспечением;

- изучением принципов установки и настройки современных межсетевых экранов на примере Comodo free firewall.

- получением знаний о международных стандартах, ГОСТах и федеральных законах Российской Федерации в области защиты информации.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: Лекция, Лабораторная работа.

Программой дисциплины предусмотрены следующие виды контроля: промежуточная аттестация в форме Экзамен (8 семестр).

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часов. Программой дисциплины предусмотрены лекционные (32 часов), практические (0 часов), лабораторные (32 часов) занятия и (44 часов) самостоятельной работы студента.

Приложение 2
к рабочей программе дисциплины
«Методы и средства защиты компьютерной информации»

Прикрепленные файлы

Примеры вопросов.docx

Примеры вопросов, задаваемых в рамках контроля:

1. Характеристика стандарта ГОСТ Р ИСО/МЭК 15408.
2. Статические и динамические методы биометрической идентификации.
3. Протокол аутентификации Kerberos, принцип работы, основные понятия.
4. Односторонняя хэш-функция. дайджест сообщения, применение совместно с ЭЦП.
5. Вредоносное ПО – категории угроз.
6. Распределенные СОА (distributed IDS), принцип работы, основные подсистемы.