Автономная некоммерческая организация дополнительного профессионального образования «Академия бизнеса и инновационных технологий»

«УТВЕРЖДАЮ»
Директор
Никишина О.Ю.
«02» октября 2017 г.

Рабочая программа
дисциплины

«Методы и средства защиты компьютерной информации»

Дополнительная профессиональная программа
по переподготовке

«Системное администрирование и информационные технологии»

Квалификация выпускника
Специалист по информационным системам

Форма обучения
очно-заочная, заочная

Москва, 2017

Составитель (и): Никишин Сергей Анатольевич

Рецензент (ы): Ольховиков Леонид Александрович

Рассмотрена и одобрена на заседании Педагогического совета
Протокол № 1/ПС от 02.10.2017

1. Цели и задачи освоения дисциплины

Цель реализации программы состоит в изучении основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи:

- ознакомление слушателей с основными методами и средствами защиты компьютерной информации;
- ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области;
- обеспечение базовой подготовки, необходимой для защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

2. Место дисциплины в структуре ДПП

Данная дисциплина входит в совокупность дисциплин необходимых для подготовки слушателя к выполнению нового вида профессиональной деятельности в области администрирования информационных систем.

Для освоения дисциплины необходимы компетенции, сформированные у обучающихся в результате изучения таких дисциплин как «Сети ЭВМ и телекоммуникации», «Компьютерные сети», «Архитектура вычислительных систем», «Автоматизированные информационные технологии», «Сетевые информационные технологии».

Освоение данной дисциплины необходимо (как предшествующее) для изучения такой дисциплины как «Технология разработки программного обеспечения».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины формируются следующие профессиональные компетенции:

- готовность к использованию основных моделей информационных технологий и способов их применения для решения задач в предметных областях (ПК-2);
- - готовность к использованию современных системных программных средств: операционных систем, операционных и сетевых оболочек, сервисных программ (ПК-5).

В результате освоения дисциплины слушатель должен:

•Знать:

- проблемы защиты информации, стоящие перед современной вычислительной техникой: вопросы административного и организационно-правового обеспечения защиты информации;

- основные системы защиты информации в России и в ведущих зарубежных странах;

- основные методологические положения защиты информации;

- основные программно-аппаратные средства защиты компьютеров и программ;

- общие вопросы обеспечения информационной безопасности при работе в сети;

- особенности защиты информации в СУБД.

•Уметь:

- ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему;

- организовывать регистрацию пользователей в сетевой операционной системе;

- организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа, организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети;

- использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.

•Владеть:

- навыками правильного выбора решений при разработке средств защиты информации.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 52 часа.

4.1. Объем дисциплины и виды учебной деятельности

Очно-заочная форма обучения

Вид учебной работы	Всего часов
Общая трудоемкость дисциплины	52
Аудиторные занятия:	40
Лекции (Л)	20
Практические занятия (ПЗ)	20
Самостоятельная работа	12
Вид итогового контроля	Экзамен

Заочная форма обучения с применением дистанционных технологий

Вид учебной работы	Всего часов
Общая трудоемкость дисциплины	52
Аудиторные занятия:	32

Лекции (Л)	12
Практические занятия (ПЗ)	20
Самостоятельная работа	20
Вид итогового контроля	Экзамен

4.2. Разделы дисциплины и виды занятий

Очно-заочная форма обучения

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу и трудоемкость (в часах)			Формы текущего контроля успеваемости
		лекции	Практические занятия/ семинары	самостоятельная работа	
1	Основные понятия и определения, концептуальные основы информационной безопасности и защиты информации	4	-	2	-
2	Правовые и организационные аспекты безопасности информационных технологий	4	-	2	-
3	Математические основы безопасности информационных технологий	6	10	4	-
4	Программно-аппаратные средства защиты информации в компьютерных системах и сетях	6	10	4	Реферат
ВСЕГО часов		20	20	12	Экзамен

Заочная форма обучения с применением дистанционных технологий

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу и трудоемкость (в часах)			Формы текущего контроля успеваемости
		лекции	Практические занятия/ семинары	самостоятельная работа	
1	Основные понятия и определения, концептуальные основы информационной безопасности и защиты	2	-	4	-

	информации				
2	Правовые и организационные аспекты безопасности информационных технологий	2	-	4	-
3	Математические основы безопасности информационных технологий	4	10	6	-
4	Программно-аппаратные средства защиты информации в компьютерных системах и сетях	4	10	6	Реферат
ВСЕГО часов		12	20	20	Экзамен

4.3. Тематическое содержание дисциплины

Раздел 1. Основные понятия и определения, концептуальные основы информационной безопасности и защиты информации.

Исторические аспекты и современная постановка задач обеспечения информационной безопасности и защиты информации, взаимосвязь проблем ИБ с развитием информационно-телекоммуникационных технологий и процессами глобализации. Национальная стратегия обеспечения ИБ в соответствии с доктриной ИБ РФ. Направления защиты информации: конфиденциальность, целостность, доступность. Основные понятия и определения: угроза, уязвимость, атаки, риски. Структура классификации, основные виды и примеры угроз в компьютерных системах. Источники и формы информационных атак. Принципы защиты информации.

Раздел 2. Правовые и организационные аспекты безопасности информационных технологий.

Правовая база защиты информации. Основные российские законы, определяющие правовую базу защиты информации: конституция РФ; закон об информации, информационных технологиях и защите информации; закон о государственной тайне, закон о защите персональных данных; закон о защите программ для ЭВМ и баз данных. Сертификация и лицензирование в сфере защиты информации: основные регламентирующие документы и ответственные органы. Проблемы борьбы с киберпреступностью.

Административный уровень защиты информации. Понятие политики ИБ, уровни разработки политики, цели и задачи. Связь программы ИБ с жизненным циклом информационных систем. Понятие о стандарте ISO 17799. Управление рисками ИБ: общее понятие, действия по отношению к рискам, этапы управления рисками. Базовый уровень безопасности. Модели и методики анализа угроз и оценки рисков. Обеспечение базовой безопасности. Понятие о двухфакторном и трехфакторном подходе к оценке рисков. Автоматизированные технологии управления ИБ (на примере COBRA, CRAMM, Digital Office и др.).

Процедурный уровень защиты информации. Цели и задачи процедурного уровня. Управление персоналом с учетом требований защиты информации в информационных системах. Направления физической защиты. Обеспечение работоспособности информационных систем. Реагирование на инциденты и планирование восстановительных работ: основные задачи и принципы организации процессов.

Стандарты и спецификации в области безопасности информационных технологий. Исторические аспекты развития - «Оранжевая книга». Система руководящих документов Гостехкомиссии России по защите информации от несанкционированного доступа в автоматизированных системах (АС) и средствах вычислительной техники (СВТ).

Структура современной международной и отечественной системы стандартов и спецификаций по безопасности информационных технологий.

Критерии оценки безопасности информационных технологий ISO15408 (ГОСТ Р ИСО/МЭК 15408): назначение и суть методологии, основные понятия, профиль защиты и задание по безопасности, структура требований, принципы оценки. Примеры разработанных профилей защиты.

Обзор стандартных требований и рекомендаций по защите информационных систем. Защита информационных систем персональных данных.

Раздел 3. Математические основы безопасности информационных технологий.

Основы криптографии. Основные понятия криптографии. Формальные модели шифров. Принципы замены и перестановки. Симметричное шифрование. Обзор исторических шифров. Понятие о стеганографии. Атаки на шифры. Понятие о линейном и дифференциальном криптоанализе. Теоретическая и практическая стойкость шифров. Поточные и блочные шифры. Примеры современных симметричных шифров и их свойства.

Принципы асимметричной криптографии: понятие об односторонних функциях и математических задачах, лежащих в основе асимметричного шифрования. Примеры алгоритмов асимметричного шифрования.

Криптографические хеш-функции: общее понятие и их применение. Ключевые и бесключевые функции, их назначение, свойства, принципы построения, примеры.

Криптографические протоколы: общее понятие, свойства, примеры. Доказательство с нулевым разглашением и протоколы аутентификации. Открытое распределение ключей - протокол Диффи-Хелмана.

Электронная цифровая подпись (ЭЦП). Понятие и назначение ЭЦП. Сходство и различия ЭЦП и собственноручной подписи. Протоколы электронной подписи: общее понятие, свойства, способы реализации и примеры схем. Понятие о ГОСТ 34.10-2001. Инфраструктура открытых ключей (PKI). Спецификации X509. Обеспечение юридической значимости электронных документов на основе закона об ЭЦП.

Протоколы электронных платежей: виды, свойства, требования безопасности, математические модели электронных денег, примеры схем и их применение в платежных системах.

Математические модели компьютерной безопасности. Математическое моделирование политик безопасности: субъектно-объектный подход, доступы,

монитор безопасности, доверенная вычислительная база. Общий обзор моделей. Примеры их реализации в ОС и СУБД.

Дискреционные модели безопасности. Модель Хариссона-Рузо-Ульмана (HRU): основные понятия, теоремы безопасности для HRU. Модель распространения прав «take-grant»: назначение, общая структура, анализ распространения прав доступа, обзор теорем безопасности.

Мандатные модели безопасности. Модель Белла-Лападула (БЛМ). Основная теорема безопасности в БЛМ. Модификации БЛМ.

Ролевые модели управления (RBAC). Общая структура моделей, принципы построения, реализация иерархии и ограничений в ролевых моделях.

Модели контроля целостности: модель Биба, неформальная модель Кларка-Вилсона.

Раздел 4. Программно-аппаратные средства защиты информации в компьютерных системах и сетях.

Общий обзор методов и средств программно-технического уровня. Место программно-технического уровня в системе комплексной технологии защиты информации. Особенности современных корпоративных информационных систем с точки зрения безопасности. Уязвимости, классификация, динамика и актуализация сведений об уязвимостях. Виды атак, механизмы и примеры их реализации. Структура многоуровневой эшелонированной защиты компьютерных систем и сетей. Обзор основных сервисов безопасности

Технологии аутентификация и управление доступом. Основные способы аутентификации. Парольные схемы, их достоинства и недостатки. Оценка стойкости парольных схем, способы повышения их надежности. Протоколы аутентификации. Система аутентификации Kerberos. Применение биометрических и комбинированных технологий аутентификации. Системы разграничения доступа. Предотвращение несанкционированных модификаций программ и данных. Защита от копирования. Обзор тиражных программно-аппаратных решений.

Защита периметра и межсетевые экраны. Общее понятие, решаемые задачи, основные защитные механизмы, классы межсетевых экранов. Примеры программных и программно-аппаратных реализаций.

Обеспечение безопасности при передаче данных. Защищенные протоколы сетевого взаимодействия. Средства защиты электронной почты. Понятие о виртуальных частных сетях. Обзор используемых программных и программно-аппаратных решений.

Аудит безопасности. Методы и средства анализа защищенности компьютерных систем и сетей. Сканеры безопасности и их возможности. Автономные и встроенные средства анализа защищенности. Системы обнаружения вторжений: общее понятие, принципы функционирования и примеры технологических решений.

Защита от вредоносного программного обеспечения._Виды и особенности вредоносных программ. Принципы организации антивирусной защиты. Обзор современных средств антивирусной защиты.

Резервное копирование. Стандартные требования к системам контроля целостности в автоматизированных системах. Обзор методов и средств контроля целостности. Технологии резервного копирования.

Обеспечение доступности информации в компьютерной среде. Направления поддержания высокой доступности: повышение отказоустойчивости и надежного оперативного восстановления. Эффективность информационных услуг. Понятие отказа. Формальные модели анализа доступности. Основные принципы и группы мер, направленные на обеспечение доступности.

5. Образовательные технологии, применяемые при освоении дисциплины

Для обеспечения качественного образовательного процесса применяются следующие образовательные технологии:

- традиционные: лекции, практические занятия;
- инновационные: интерактивные лекции (в режиме on-line и /или off-line);
- интерактивные: вебинары, чат, форумы, интернет-конференции;
- самостоятельная работа слушателей.

К интерактивным методам относятся также презентации с использованием различных вспомогательных средств: интерактивной доски, раздаточных материалов, видеофильмов, слайдов, мультимедийной презентации и т.п.

Интерактивные методы поощряют активное участие каждого в учебном процессе;

- способствуют эффективному усвоению учебного материала;
- оказывают многоплановое воздействие на обучающихся;
- осуществляют обратную связь (ответная реакция аудитории);
- формируют у обучающихся мнения и отношения; формируют жизненные навыки;
- способствуют изменению поведения.

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

Основными видами самостоятельной работы являются:

- выполнение индивидуальных заданий,
- изучение основной и дополнительной литературы,
- поиск и сбор информации по дисциплине в периодических печатных и интернет-изданиях.

6.1. Примерный перечень вопросов для подготовки к экзамену

1. Компьютерная информация: определение, основные категории с точки зрения безопасности.
2. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности. Критерии надежности систем, классы безопасности.
3. Политика безопасности информационных систем и ее основные элементы.
4. Классификация угроз информационным системам.

5. Обзор нормативных правовых актов РФ в области информационной защиты.
6. Дискреционный и мандатный доступ к ресурсам информационных систем.
7. Основные методы обеспечения безопасности информационных систем.
8. Основные услуги безопасности, предоставляемые информационными системами.
9. Механизмы реализации услуг безопасности в информационных системах.
10. Классификация криптографических алгоритмов.
11. Структурная схема симметричной криптосистемы.
12. Структурная схема асимметричной криптосистемы.
13. Математические определения шифра, процедур шифрования и дешифрации.
14. Понятие секретности криптоалгоритма. Разновидности атак на криптоалгоритмы.
15. Принцип итерирования как основной принцип построения современных блочных шифров. SP-сеть, сеть Фейштеля.
16. Блочное симметричное шифрование, обратимые и необратимые, линейные и нелинейные преобразования.
17. Криптоатаки на поточные шифры, построение ЛРС с последовательностями наибольшей длины.
18. Методы построения нелинейных поточных шифров.
19. Асимметричные криптосистемы: принципы функционирования, трудновычислимые математические задачи, определяющие криптостойкость асимметричных криптоалгоритмов.
20. RSA: возможные криптоатаки и криптостойкость алгоритма.
21. RSA: математические основы криптоалгоритма.
22. RSA: структура криптоалгоритма.
23. Алгоритм асимметричного шифрования Рабина.
24. Криптосистема ЭльГемаля: структура, криптостойкость.
25. Метод ключевого обмена Диффи-Хелмана.
26. Системы управления ключами: разновидности ключей, схемы обмена ключами.
27. Сертификация открытых ключей асимметричных алгоритмов. Инфраструктура PKI.
28. Хэш-функции: назначение и основные свойства.
29. Итеративно-последовательная схема построения хэш-функций. Хэш-функции на основе блочных шифров.
30. Система ЭЦП на основе алгоритма ЭльГемаля.
31. Система ЭЦП на основе эллиптических кривых.
32. Электронная цифровая подпись: назначение, структура системы ЭЦП на основе алгоритма RSA.
33. Генерация криптостойких случайных чисел.
34. Вероятностная генерация простых чисел для криптоалгоритмов.
35. Аутентификация в информационных системах: назначение, разновидности, угрозы подсистемам аутентификации.

36. Биометрические методы аутентификации пользователей.
37. Системы аутентификации с защищенными паролями и с проверкой на стороне сервера.
38. Система аутентификации по схеме «запрос-ответ».
39. Протокол аутентификации пользователей Kerberos.
40. Угрозы безопасности в глобальных сетях.
41. Межсетевые экраны: назначение, основные функции, состав.
42. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостатки.
43. Proxy-сервера: назначение, основные функции, достоинства и недостатки.
44. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона.
45. Обзор криптографических протоколов: SSL, TLS, IPSecurity, SSH, PPTP, L2TP.
46. Обзор аутентификационных протоколов: PAP,CHAP, EAP, RADIUS.
47. Вредоносные программы: определение, классификация.
48. Эксплойты: определение. Атаки на переполнение буфера и методы защиты от них.
49. Эксплойты: определение. SQL-инъекции и методы защиты от них.
50. Компьютерные вирусы: определение, методы заражения и маскировки. Методы защиты от вирусов.

6.2. Примерная тематика рефератов

1. Режимы шифрования блочных шифров ECB, CBC, CFB, OFB.
2. Алгоритм шифрования TEA: структура, достоинства и недостатки.
3. Алгоритм шифрования DES: структура, достоинства и недостатки.
4. Линейный криптоанализ блочных шифров.
5. Дифференциальный криптоанализ блочных шифров.
6. Поточные шифры: принципы функционирования, структура.
7. Средства аудита ОС семейства Windows .
8. Модель безопасности ОС семейства Windows.
9. Подсистема аудита ОС семейства Unix.
10. Модель безопасности ОС Unix.

6.3. Типовые контрольные задания или иные материалы, необходимые для оценки результатов самостоятельной работы

1. Какие структуры, которые вносятся в неопределяемый объект под названием информация?
2. На использовании какого метода основано решение задач анализа, проектирования, создания и поддержки в рабочем состоянии сложных систем?
3. Как осуществляется иерархическая декомпозиция вычислительной системы?
4. В чем заключается иерархическое представление информации в вычислительных системах?

5. К каким результатам приводит появление незаконных информационных потоков?
6. Что служит мерой опасности незаконного канала передачи информации?
7. Что можно противопоставить взлому системы защиты информации?
8. Как реализуется мандатный контроль?
9. Как понимается обеспечение безопасности информации в документах Гостехкомиссии России?
10. Чем занимается криптография?
11. Что такое криптографическая система?
12. Сформулируйте определение шифра.
13. Чем отличаются блочные и поточные криптосистемы?
14. Какие требования предъявляются к блочным шрифтам?
15. Какие преобразования шифра выполняются при операции рассеивания?
16. Какие шифры называются послойными?
17. В чем сущность идеи многократного шифрования?
18. Какой признак присущ активной атаке, при использовании самосинхронизирующихся шифров?
19. Как работают поточные криптосистемы?
20. С какой целью осуществляется идентификация пользователей компьютерных систем?
21. Какую функцию выполняют пароли в системах защиты компьютерной информации?
22. Укажите основные атрибуты цифровых сертификатов?
23. Для чего используются цифровые сертификаты?
24. Как называется система проверки цифровых сертификатов?
25. Для чего применяется брандмауэр?
26. Укажите назначение демилитаризованной зоны?
27. Укажите виды брандмауэров?
28. Сколько существует уровней контроля не декларируемых возможностей?
29. Какие показатели являются результатами контроля исходного состояния ПО?
30. С какой целью проводится проверка на отсутствие недекларируемых возможностей средств защиты информации?
31. С какой целью в программное обеспечение вводятся программные закладки?
32. Какие задачи решаются при проведении сертификационных испытаний?
33. Что является методологической основой для исследований, выполняемых при проведении сертификационных испытаний?
34. Что представляет собой комплексная система защиты информации?
35. Назовите главную функцию комплексной системы защиты информации?
36. Каким требованиям должна отвечать комплексная система защиты информации?
37. В чем заключается анализ общей проблемы безопасности?
38. Какими средствами обеспечивается защита компьютерных систем?

6.4. Примерный перечень лабораторных работ

Лабораторная работа № 1. Опишите информационную среду для перечисленных объектов и укажите для нее возможные информационные угрозы:

а) школа;
б) библиотека;
в) ваша семья;
г) супермаркет;
д) кинотеатр;
е) любая другая среда на ваш выбор.

Требования. Проект должен удовлетворять следующим требованиям к содержанию:

- представлять собой единое логически связанное целое;
- обеспечить полноту представления материала.

Критерии оценивания:
- полнота и системность представленных данных;
- самостоятельность разработки.

Оценивание – зачет, незачет.

Лабораторная работа № 2. Аутентификация пользователей Web-систем ссредствами технологии PHP

1. Цель работы: изучение принципов аутентификации пользователей в Web-системах на примере PHP-сеансов.

2. Порядок выполнения работы:
- Изучить принципы аутентификации пользователей в Web-системах.
- Реализовать систему аутентификации с помощью PHP-сеансов

3. Содержание отчета:
1) титульный лист;
2) формулировка цели работы;
3) описание результатов выполнения;
4) выводы, согласованные с целью работы.

Оценивание – зачет, незачет.

Лабораторная работа № 3. Защита информации с помощью пароля.

1. Цель работы: исследование защиты информации с применением пароля, а также исследование методов противодействия атакам на пароль.

2. Порядок выполнения работы:

2.1. Проведение атаки перебором (bruteforce attack):

Используя программу для вскрытия паролей произвести атаку на зашифрованный файл try_me.rar (try_me.arj, try_me.zip).

Область перебора – все печатаемые символы, длина пароля от 1 до 4 символов.

Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым.

Выполнив пункт 1, сократить область перебора до фактически используемого (например если пароль 6D1A – то выбрать прописные английские буквы и цифры).

Провести повторное вскрытие.

Сравнить затраченное время.

2.2. Проведение атаки по словарю (dictionary attack)

Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например love, god, table, admin и т.д.).

Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

Попытаться определить пароль методом прямого перебора.

Сравнить затраченное время.

3. Содержание отчета:

1) титульный лист;
2) формулировка цели работы;
3) описание результатов выполнения;
4) выводы, согласованные с целью работы.

Оценивание – зачет, незачет.

Лабораторная работа № 4.

1. Цель работы: ознакомиться с основными методами криптографической защиты информации и получить практические навыки создания ПО по криптографическим преобразованиям информации.

2. Порядок выполнения работы:

На языке C++ или Pascal написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

3. Содержание отчета:

1) название работы;
2) цель работы;
3) тексты программ.
4) общие выводы, сделанные в процессе выполнения лабораторной работы.

Оценивание – зачет, незачет.

Критерии оценивания учебной деятельности слушателя

Критерии оценки учебной деятельности слушателя при работе над рефератом по обсуждаемому вопросу

Оценка	Характеристики ответа слушателя
Отлично	- слушатель глубоко и всесторонне усвоил проблему; - последовательно и грамотно ее излагает; - опираясь на знания основной и дополнительной литературы, - обосновывает и аргументирует выдвигаемые им идеи; - делает квалифицированные выводы и обобщения.
Хорошо	- слушатель твердо усвоил тему, по существу излагает ее, опираясь на знания основной литературы; - не допускает существенных неточностей; - делает выводы и обобщения.
Удовлетворительно	- тема раскрыта недостаточно четко и полно, то есть слушатель освоил проблему, по существу излагает ее, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - затрудняется в формулировании выводов и обобщений.
Неудовлетворительно	- слушатель не усвоил значительной части проблемы; - допускает существенные ошибки и неточности при рассмотрении ее; - не формулирует выводов и обобщений.

Критерии оценки уровня овладения слушателем компетенциями на этапе экзамена по учебной дисциплине

Оценка	Характеристики ответа студента
Отлично	слушатель самостоятельно и правильно ответил на поставленные вопросы, уверенно, логично, последовательно и аргументировано излагал свой ответ, используя основные понятия, ссылаясь на примеры из практики, положения теории.
Хорошо	слушатель самостоятельно и в основном правильно ответил на поставленные вопросы, уверенно, логично, последовательно и аргументировано излагал свой ответ, используя основные понятия, ссылаясь на положения теории.
Удовлетворительно	слушатель самостоятельно и в основном представил ответ на поставленные вопросы, допустил несущественные ошибки, слабо аргументировал свое решение, используя общие определения и понятия.
Неудовлетворительно	слушатель не представил ответов на поставленные вопросы.

Критерии оценки учебных действий студентов по решению задач и заданий в рамках контрольных работ

Оценка	Характеристики ответа
Отлично	слушатель самостоятельно и правильно решил учебно-профессиональную задачу или задание
Хорошо	слушатель самостоятельно и в основном правильно решил учебно-профессиональную задачу или задание

Удовлетворительно	слушатель в основном решил учебно-профессиональную задачу или задание, допустил несущественные ошибки
Неудовлетворительно	слушатель не решил учебно-профессиональную задачу или задание.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Гуц А.К. Теория игр и защита компьютерных систем [Электронный ресурс]: учебное пособие/ Гуц А.К., Вахний Т.В.— Электрон. текстовые данные.— Омск: Омский государственный университет им. Ф.М. Достоевского, 2013.— 160 с.— Режим доступа: http://www.iprbookshop.ru/24947.— ЭБС «IPRbooks», по паролю.

2. Метелица Н.Т. Вычислительные сети и защита информации [Электронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. текстовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю.

3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks», по паролю.

б) дополнительная литература:

1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks», по паролю.

2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]: учебное пособие для вузов/ Девянин П.Н.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2013.— 338 с.— Режим доступа: http://www.iprbookshop.ru/12000.— ЭБС «IPRbooks», по паролю.

3. Игнатова Е.В. Язык информационных технологий [Электронный ресурс]: учебное пособие/ Игнатова Е.В.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 75 с.— Режим доступа: http://www.iprbookshop.ru/11143.— ЭБС «IPRbooks», по паролю.

4. Ковалева Н.Н. Информационное право России [Электронный ресурс]: учебное пособие/ Ковалева Н.Н.— Электрон. текстовые данные.— М.: Дашков и К, Ай Пи Эр Медиа, 2012.— 352 с.— Режим доступа: http://www.iprbookshop.ru/5995.— ЭБС «IPRbooks», по паролю.

5. Исакова А.И. Информационные технологии [Электронный ресурс]: учебное пособие/ Исакова А.И., Исаков М.Н.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2012.— 174 с.— Режим доступа: http://www.iprbookshop.ru/13938.— ЭБС «IPRbooks», по паролю.

6. Малюк А.А. Этика в сфере информационных технологий [Электронный ресурс]: монография/ Малюк А.А., Полянская О.Ю., Алексеева И.Ю.—

Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 344 с.— Режим доступа: http://www.iprbookshop.ru/12070.— ЭБС «IPRbooks», по паролю.

7. Методы решения специальных задач с использованием информационных технологий [Электронный ресурс]: практикум/ — Электрон. текстовые данные.— М.: Московский государственный строительный университет, Ай Пи Эр Медиа, ЭБС АСВ, 2014.— 133 с.— Режим доступа: http://www.iprbookshop.ru/27893.— ЭБС «IPRbooks», по паролю.

8. Некраха А.В. Организация конфиденциального делопроизводства и защита информации [Электронный ресурс]: учебное пособие/ Некраха А.В., Шевцова Г.А.— Электрон. текстовые данные.— М.: Академический Проект, 2015.— 222 с.— Режим доступа: http://www.iprbookshop.ru/36849.— ЭБС «IPRbooks», по паролю.

9. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 544 с.— Режим доступа: http://www.iprbookshop.ru/7943.— ЭБС «IPRbooks», по паролю.

10. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) [Электронный ресурс]: учебное пособие для вузов/ Шелухин О.И., Сакалема Д.Ж., Филинова А.С.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2013.— 220 с.— Режим доступа: http://www.iprbookshop.ru/37191.— ЭБС «IPRbooks», по паролю.

в) интернет-ресурсы:

1. http://www.compulenta.ru/ – Интернет-издание «Компьюлента», посвященное новостям компьютерной индустрии, науки и техники.
2. http://www.wisesoft.ru/ – Каталог журналов (большой выбор компьютерных журналов).
3. http://inf1.info/ – Планета информатики.
4. http://www.teachvideo.ru/faq – Коллекция видеоуроков по разным сферам IT-тематики.
5. http://www.spohelp.ru/ – Пакет свободного программного обеспечения для образовательных учреждений РФ.
6. http://www.intuit.ru/ – Интернет университет информационных технологий.
7. http:///newb.by.ru/index.html – Учебные языки программирования.

8. Материально-техническое обеспечение дисциплины

Учреждение располагает материально-технической базой, обеспечивающей проведение всех видов лекционных, семинарских и практических занятий.

Слушатели имеют доступ с компьютеров, входящих в локальную сеть и сеть Wi-Fi, в Интернет.

В Учреждении организованы учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического

обслуживания учебного оборудования. Данные аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа используются слайд-лекции с обратной связью (интерактивные).

9. Методические указания слушателям по освоению дисциплины

Методические указания для слушателей по организации самостоятельной работы в процессе освоения дисциплины

Самостоятельная работа имеет целью закрепление и углубление знаний и навыков, полученных на лекциях и семинарских занятиях по дисциплине, подготовку к экзамену, а также формирование культуры умственного труда и самостоятельности в поиске и приобретении новых знаний.

Основными видами самостоятельной работы являются:

- изучение отдельных теоретических вопросов при подготовке к семинарам, в том числе подготовка докладов, сообщений, рефератов по данным вопросам;
- осмысление информации, сообщаемой преподавателем, ее обобщение и краткая запись;
- своевременная доработка конспектов лекций;
- подбор, изучение, анализ и конспектирование рекомендуемой литературы;
- подготовка к экзамену.

Методические рекомендации по выполнению рефератов

Выбор темы и назначение руководителя. Тема реферата выбирается слушателем самостоятельно из предоставленного преподавателем перечня или формулируется самостоятельно и согласовывается с преподавателем.

Подбор и изучение литературы. При написании реферата целесообразно использовать не только учебники и учебные пособия, но и монографии, диссертации, справочники, словари, журнальные статьи, сборники научных трудов, материалы научных конференций и др. Большую помощь в подготовке реферата может оказать сеть Интернет, где также можно получить нужную информацию.

Изучение литературы предполагает выделение основных идей и письменную фиксацию всего ценного в их содержании, для чего нужно владеть начальными навыками работы с текстом. Чтобы лучше понять логику изучаемого текста, надо составить развернутый план, с помощью которого легко восстановить в памяти идеи автора. Это логический каркас исследования проблемы, которым можно воспользоваться при составлении плана собственной работы. План может быть простым, т.е. состоящим их общих заголовков крупных частей текста, или сложным, развернутым, включающим в виде пунктов и подпунктов дробные логически взаимосвязанные положения.

Структура и объём. Структура реферата состоит из следующих элементов:

1. Титульный лист.
2. Оглавление.
3. Введение.
4. Основная часть, состоящая из глав (параграфов).
5. Заключение.
6. Библиография (список использованной литературы).

Во Введении (1-2 страницы) обосновывается актуальность темы, кратко излагаются известные подходы к ее изучению в литературе, формулируются цели и задачи написания работы. Основное часть работы включает в себя материал, призванный отразить центральные вопросы выбранной темы. Заключение (1-2 страницы) должно содержать основные выводы, к которым пришел слушатель, работая над избранной темой.

Объем реферата не должен превышать 15-20 печатных страниц формата А4.

Общие требования к стилю изложения. Реферат должен быть выдержан в стиле научного текста, для которого характерны точность, лаконичность, аргументированность и доказательность. Правомерно использование определённых фразеологических оборотов, слов-связок, вводных слов, которые логически связывают предыдущую и последующую части текста. Без необходимости в текст не стоит вводить слова иностранного происхождения. В тексте не должно быть витиеватых оборотов, повторов, терминов и слов, точное значение которых слушателю неизвестно.

Библиография. Библиография, т.е. список использованной литературы, помещается после заключения. Список формируется в алфавитном порядке (по фамилиям авторов и заглавиям книг) и нумеруется. Авторы, носящие одинаковую фамилию, располагаются в алфавитном порядке по инициалам. Работы одного и того же автора располагаются в алфавитном порядке по заглавиям или в хронологическом порядке по годам издания.

Оформление печатного текста. Реферат принимается только в печатном виде. Его текст выполняется шрифтом «Times New Roman», размер шрифта – 14, межстрочный интервал – полуторный, нумерация страниц – вверху, от центра (номер на титульном листе не ставится), поля: верхнее – 2 см, нижнее – 2 см, правое – 1 см, левое – 3 см.

Все структурные элементы текста, кроме параграфов внутри глав, начинаются с новой страницы. Главы и параграфы должны иметь заголовки.

Листы реферата сшиваются в папке-скоросшивателе.