Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Московский государственный институт культуры»

УТВЕРЖДАЮ
Декан факультета СГФ
_____К.В. Ивина
«26» октября 2015 г.

УТВЕРЖДАЮ
Зав. кафедрой документоведения и архивоведения
_____О.Н. Кокойкина
«28» сентября 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки

Документоведение и архивоведение

Профиль подготовки

Документоведение и документационное обеспечение управления

Квалификация (степень) выпускника

Бакалавр

Форма обучения

Очная, заочная

Согласовано:
*С председателем методического совета по качеству по направлению «Документоведение и архивоведение» О.Н. Кокойкиной*_____

Москва - 2015

1. Цели освоения дисциплины

1. Цели освоения учебной дисциплины

Целью изучению дисциплины «Информационная безопасность и защита информации» является изучение теоретических и практических проблем информационной безопасности и защиты информации», а также проектирование и использование систем защиты информации, их применение в профессиональной деятельности.

Основные задачи

ознакомление с теоретическими аспектами защиты информации;

ознакомление с информационными технологиями, обеспечивающими информационную безопасность и защиту информации;

ознакомление со способами разработки средств информационной безопасности и защиты информации;

применение средств информационной безопасности и защиты информации в профессиональной деятельности.

2. Место дисциплины в структуре ООП ВО

Дисциплина относится к Базовой части Блока 1 «Дисциплины (модули)» подготовки бакалавра по направлению «Документоведение и архивоведение» в соответствии с ООП ВО. Дисциплина осваивается на 3 курсе, в 5 и 6 семестрах.

Знания, полученные при изучении дисциплины «Информационная безопасность и защита информации» могут быть использованы при прохождении учебных практик, а также при выполнении выпускной работы по направлению подготовки «Документоведение и архивоведение».

Основные предметы, с которыми тесно взаимосвязана тематика дисциплины: «Информационные технологии» (изучается параллельно, в 5 и 6 семестрах) и Информатика (изучалась во 2 семестре).

Требования к содержанию курса

Предпосылки формирования сферы знаний по информационной безопасности; основные меры, направленные на обеспечение ИБ на различных уровнях деятельности; значение информационной безопасности для документоведения и архивоведения, перспективы развития технологий обеспечения информационной безопасности.

3. Формируемые компетенции

В результате освоения дисциплины студент должен овладеть следующими компетенциями:

- способность к использованию основных методов, способов и средств получения, хранения, переработки информации (ОК-10);
- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-6);
- владение методами защиты информации (ПК-17).

4. Знания, умения и навыки, получаемые в результате освоения дисциплины

В результате изучения дисциплины студенты должны

В результате освоения дисциплины студент должен:

знать:

- основные понятия информационной безопасности;
- основные направления защиты информации;
- законодательство Российской Федерации в области защиты информации;
- современные методы и средства защиты информации в информационно-телекоммуникационных системах;
- архитектуру защищённых систем документооборота.

уметь:

- разрабатывать политику информационной безопасности;
- проводить оценку угроз безопасности объекта информатизации;
- реализовывать простые информационные технологии реализующие методы защиты информации;
- применять методики оценки уязвимости в информационно-телекоммуникационных сетях;
- проектировать системы защиты информации.

владеть:

- методами защиты информации;
- средствами защиты информации в сетях ЭВМ;
- навыками программирования алгоритмов криптографической защиты информации.

5. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов, из них 66 аудиторных: 34 часа лекций (18 – в 5 семестре, 16 – в 6 семестре), 32 часа семинаров (18 часов – в 5 семестре, 14 часов – в 6 семестре), и 114 часов самостоятельной работы (18 часов – в 5 семестре, 96 часов – в 6 семестре).

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				**Формы текущего контроля успеваемости *(по неделям семестра)*** **Форма промежуточной аттестации *(по семестрам)***
				Всего	Лекции	Семинары, практич. раб.	Самост. раб.	
1	Понятие и составляющие информационной безопасности	5	1	6	2	2	2	Опрос
2	Теоретические основы методов защиты информационных систем	5	2	6	2	2	2	Опрос
3	Криптографические методы защиты информации	5	3	6	2	2	2	Опрос
4	Стандарты и спецификации в области информационной безопасности	5	4	6	2	2	2	Опрос
5	Организационный уровень информационной безопасности	5	5	6	2	2	2	Опрос
6	Угрозы информационной безопасности в компьютерных системах	5	6	6	2	2	2	Опрос Практикум
7	Программно-технический уровень информационной безопасности	5	7	6	2	2	2	Опрос Практикум

8	Защита информации от утечки по техническим каналам	5	8	6	2	2	2	Опрос Практикум
9	Защита информации от несанкционированного доступа	5	9	6	2	2	2	Опрос
	Итого:			54	18	18	18	Зачет
10	Вирусы как угроза информационной безопасности	6	1	16	2	2	12	Опрос
11	Средства антивирусной защиты	6	2	16	2	2	12	Опрос
12	Специфика технологии защищенного документооборота	6	3	16	2	2	12	Опрос
13	Технологии обработки конфиденциальных документов: обработка документов входного потока	6	4	16	2	2	12	Опрос
14	Технологии обработки конфиденциальных документов: обработка документов выходного и внутреннего потоков	6	5	16	2	2	12	Опрос
15	Технологии архивного хранения конфиденциальных документов и дел	6	6	16	2	2	12	Опрос
16	Технологии и порядок предоставления конфиденциальной	6	7	16	2	2	12	Опрос

	информации и документов							
17	Мобильные технологии и проблема защиты информации	6	8	14	2	0	12	Опрос
	Итого:			126	16	14	96	Экзамен
	Всего			180	22	44	222	

Тема 1. Понятие и составляющие информационной безопасности

Лекционное занятие (2 часа)

Объекты защиты: личность; информация; материальные ценности.

Понятие «безопасная деятельность» предприятия или организации.

Ключевые термины и понятия в области ИБ и защиты информации.

Основные источники угроз информационной безопасности (промышленный шпионаж, хакеры, акты саботажа, ошибки деятельности человека, сбои оборудования, стихийные бедствия).

Типы и причины угроз безопасности информации (нарушение безопасности информации: при выполнении процедур доступа или процедур разграничения доступа, в процедурах учета действий пользователей и их программ; нарушение безопасности информации, связанные с определением грифа секретности.

Семинарское занятие (2 часа)

Категории информационной безопасности.

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 2. Теоретические основы методов защиты информационных систем

Лекционное занятие (2 часа)

Категории и базовые понятия. Классическая схема защиты и безопасности информации.

Роль методов и средств защиты информации в информационной технологии.

Синтаксические, семантические и прагматические аспекты защиты информации.

Алгебраическая система как универсальный способ логико-математической формализации алгоритмов защиты информации.

Семинарское занятие (2 часа)

Базовая схема защиты и обеспечения информации К.Шеннона

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 3. Криптографические методы защиты информации

Лекционное занятие (2 часа)

История развития криптографии.

Базовые методы криптографической защиты.

Специфика криптографии в условиях электронного документооборота.

Семинарское занятие (2 часа)

Алгоритмы криптографической защиты методом перестановок, замены и ключа.

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 4. Стандарты и спецификации в области информационной безопасности

Лекционное занятие (2 часа)

Федеральный закон РФ «О техническом регулировании».

Стандарты RSA, DES, AES

Семинарское занятие (2 часа)

Алгоритмы криптографической защиты методом замены

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 5. Организационный уровень информационной безопасности

Лекционное занятие (2 часа)

Концептуальная схема деятельности по обеспечению безопасности и защиты информации.

Модель офицера ОБИ.

Семинарское занятие (2 часа)

Алгоритмы криптографической защиты методом ключа

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 6. Угрозы информационной безопасности в компьютерных системах

Лекционное занятие (2 часа)

Классификация угроз информационной безопасности. Специфика угроз в компьютерных технологиях информационных систем.

Семинарское занятие (2 часа)

Стандарт криптографической защиты данных DES

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 7. Программно-технический уровень информационной безопасности

Лекционное занятие (2 часа)

Классификация программных средств ОБИ.

Программы защиты информации программных средств общего назначения.

Программы защиты информации базовых программных средств.

Многообразие программ защиты информации специального назначения.

Семинарское занятие (2 часа)

Новый стандарт шифрования с открытым ключом AES

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 8. Защита информации от утечки по техническим каналам

Лекционное занятие (2 часа)

Концептуальная схема утечки информации по техническим каналам. Параметры утечки. Общая характеристика средств защиты информации от утечки по техническим каналам.

Семинарское занятие (2 часа)

Поточные шифры

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 9. Защита информации от несанкционированного доступа

Лекционное занятие (2 часа)

Концептуальная схема защиты информации от несанкционированного доступа. Общая характеристика средств защиты о НСД в общих, базовых и специальных программных средствах.

Понятие ядра защиту операционной системы.

Ущербность системы Windows.

Семинарское занятие (2 часа)

Криптосистема RSA

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Зачет.

Тема 10. Вирусы как угроза информационной безопасности

Лекционное занятие (2 часа)

Классификация диверсионных программных средств: троянские кони, вирусы, черви.

Модель распространения и заращения компьютерного вируса. Основные угрозы от вирусных атак.

Примеры программ – вирусов.

Семинарское занятие (2 часа)

Алгоритмы шифрования с открытым ключом

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 11. Средства антивирусной защиты

Лекционное занятие (2 часа)

Алгоритмы работы вирусов и антивирусов. Характеристика антивирусных программ. Надежные методы защиты от вирусов.

Семинарское занятие (2 часа)

Алгоритмы цифровой подписи

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 12. Специфика технологии защищенного документооборота

Лекционное занятие (2 часа)

Обобщенная схема документооборота. Концептуальная схема защиты информации в документообороте.

Этапы документооборота и роль методов и средств защиты информации на каждом этапе.

Обобщенные параметры алгоритмов ОБЗИ в документообороте.

Семинарское занятие (2 часа)

Роль генераторов псевдослучайных последовательностей в обеспечении защиты информации

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 13. Технологии обработки конфиденциальных документов: обработка документов входного потока

Лекционное занятие (2 часа)

Понятия конфиденциальных документов.

Концептуальная схема защиты информации во входном потоке документов.

Классификация и структуризация входных документов. Защита иерархически структурированной информации.

Преимущество фасетной классификации документов. Машина Корсакова как концептуальный прототип формализации алгоритма защиты документов входного потока.

Семинарское занятие (2 часа)

Методы и средства защиты документов входного потока (на примере средства MS OFFICE).

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 14. Технологии обработки конфиденциальных документов: обработка документов выходного и внутреннего потоков

Лекционное занятие (2 часа)

Концептуальные схемы зашиты информации в сетевых, иерархических и реляционных моделях данных.

Специфика защиты информации в интеллектуальных информационных компьютерных системах.

Семинарское занятие (2 часа)

Методы и средства защиты документов внутреннего потока (на примере средства MS OFFICE).

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 15. Технологии архивного хранения конфиденциальных документов и дел

Лекционное занятие (2 часа)

Концептуальные схемы зашиты информации в сетевых, иерархических и реляционных моделях хранения данных.

Семинарское занятие (2 часа)

Методы и средства хранения конфиденциальных документов (на примере средства MS OFFICE).

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 16. Технологии и порядок предоставления конфиденциальной информации и документов

Лекционное занятие (2 часа)

Концептуальные схемы зашиты информации в сетевых, иерархических и реляционных моделях хранения.

Проблема рекламы и обеспечение безопасности информации.

Семинарское занятие (2 часа)

Методы и средства защиты документов выходного потока (на примере средства MS OFFICE).

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Тема 17. Мобильные технологии и проблема защиты информации

Лекционное занятие (2 часа)

Характеристика мобильных технологий.

Электронные цифровые подписи – новый метод обеспечения информационной безопасности в мобильных системах. Понятие электронной цифровой подписи. Принципы и условия использования электронной цифровой подписи. Обязательства владельца по принятию сертификата ключа подписи и защита персональных данных. Использование электронной цифровой подписи в сфере государственного управления и организационного управления.

Семинарское занятие (2 часа)

Алгоритмы работы с электронной цифровой подписью.

Самостоятельная работа студентов (2 часа)

Изучение материалов лекций, основной и дополнительной литературы. Подготовка к опросу.

Экзамен.

6. Образовательные технологии

Процесс обучения включает:

- лекционные аудиторные занятия;
- семинары;
- внеаудиторная самостоятельная работа: изучение текстов лекций, ознакомление с основной и дополнительной литературой, подготовка к контрольным работам и сдаче тестов, подготовка к итоговой аттестации.

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

Формы аттестации

Итоговой формой аттестации по данной дисциплине является экзамен.

Средства текущего контроля успеваемости

Практикум.

Опрос.

Тестирование.

Контрольная работа.

Виды практических занятий

Теоретические задачи по теме обеспечения безопасности информации и криптозащите.

Компьютерный практикум.

Примерный перечень контрольных вопросов

1. Понятия «информационная безопасность» и «защита информации».
2. Причины важнейшей роли информационной безопасности по сравнению с другими составляющими интегральной безопасности предприятия.
3. Основные источники угроз информационной безопасности.
4. Пассивные и активные способы реализации угроз безопасности информации.
5. Типы угроз безопасности информации.
6. Причины угроз безопасности информации.
7. Основные задачи, решение которых необходимо для защиты от НСД.
8. Классификация компьютерных преступлений.
9. Три наиболее опасные угрозы информационным системам.
10. Какой процент утечки коммерческой информации по оценке западных специалистов может привести к банкротству фирмы?
11. Основные способы перехвата и утечки информации.
12. Основные уровни обеспечения информационной безопасности.
13. Категории (грани) информации, подлежащие защите.
14. Базовые законодательные акты в области информационной безопасности.
15. Ключевые источники законодательных и нормативно-технических актов в области информационной безопасности.
16. Национальные интересы Российской Федерации в сфере информационной безопасности.
17. Основные источники государственных информационных ресурсов.
18. Виды и источники угроз национальной безопасности РФ.
19. Базовые мероприятия по обеспечению информационной безопасности РФ в сфере науки и техники.
20. Ключевые мероприятия по обеспечению информационной безопасности РФ в информационных и телекоммуникационных системах.
21. Основные составляющие руководящего документа, характеризующие политику безопасности организации.
22. Административный уровень защиты: анализ рисков для информационной системы организации.

23. Этапы работ по обеспечению информационной безопасности на административном уровне.
24. Стандарты в области разработки политики безопасности и анализа рисков.
25. Группы процедурных мер для обеспечения информационной безопасности.
26. Физические средства защиты информации.
27. Ключевые направления поддержания работоспособности компьютерных систем.
28. Основные функции программных средств по обеспечению информационной безопасности.
29. Классификация сервисов программных средств защиты информации.
30. Идентификация и аутентификация – основа программно-технических средств обеспечения безопасности.
31. Основные мероприятия по повышению надежности парольной защиты.
32. Антивирусные программные продукты.
33. Базовые организационные меры безопасности для предотвращения «вирусных» атак.
34. Криптографические средства защиты информации.
35. Различия в криптографическом и стеганографическом методах защиты информации.
36. Классы и группы защищенности средств вычислительной техники от несанкционированного доступа к информации.
37. Классификация информационных систем в РФ по уровню безопасности.
38. Основные принципы обеспечения архитектурной безопасности информационных систем.
39. Стандарты в области безопасности распределенных систем.
40. Базовые сервисы обеспечения безопасности для информационных систем.
41. Виды деятельности в области защиты информации, подлежащие лицензированию Гостехкомиссией России.
42. Основные способы реагирования на нарушения информационной безопасности.
43. Классификация сбоев и нарушений в сетях передачи информации.
44. Основные средства защиты информации в сети:
45. Система Kerberos как пример комплексного решения контроля доступа в сети.
46. Этапы организации разграничения доступа к информации в сети.
47. Основные задачи, решаемые при создании механизмов разграничения доступа к информации.

Виды контрольных работ

Проверка навыков работы с антивирусными программами.

Проверка навыков администрирования средств операционной системы.

Проверка навыков разграничения доступа к базовым программных средствам (на примере средств MS OFFICE).

Проверка навыков решения криптографических задач.

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература

1. Арутюнов, В.В. Информационная безопасность и защита информации: Учебное пособие для студентов ун-тов и вузов культуры и искусств и др. учебн. заведений /В.В.Арутюнов. - М., 2003. – 49 с. - Библиогр.: 46 назв.
2. Алешин, Л. И. Информационные технологии [Текст] : [учеб. пособие]. - М. : Литера, 2008. - 423, [1] с. : ил. - (Современная библиотека; вып. 35). - Библиогр.: с. 412-416. - ISBN 978-5-91670-005-3 : 200-.
3. Дубровин, А. Д. Интеллектуальные информационные системы : [учеб. пособие для студентов вузов]. - М. : [Б. и.], 2010. - 358 с. : схем., табл., формулы. - Библиогр.: с. 356-358. - 120- ; 283-69.
4. Информационные технологии : учебник / О. Л. Голицына, Н. В. Максимов, Т. Л. Партыка, И. И. Попов. - Изд. 2-е, перераб. и доп. - М. : Форум : Инфра-М, 2009. - 607 с. : ил., схем., табл. - Библиогр.: с. 558-560. - ISBN 978-5-91134-178-7. - ISBN 978-5-16-003207-8 : 240-46.
5. Климов, Владимир Александрович. ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ [Электронный ресурс] : Учебник / Гаврилов М.В., Климов В.А. - 4-е изд. ; пер. и доп. - М. : Издательство Юрайт, 2015. - 383. - (Бакалавр. Прикладной курс). - ISBN 978-5-9916-5784-6 : 1000.00.
6. Максимов, Н. В. Компьютерные сети [Текст] : учеб. пособие. - Изд. 2-е, испр. и доп. - М. : Форум-ИНФРА-М, 2007. - 446 с. - Библиогр.: с. 403-405. - ISBN 978-5-91134-058-2 : 350-.
7. Попов, В. Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности. - М. : Финансы и статистика, 2005. - 171, [1] с. : ил., табл. - ISBN 5-279-03007-4 : 103-.
8. Шеин, П. Д. Разработка и стандартизация программных средств и информационных технологий [Текст] : учеб. пособие / Моск. гос. ун-т культуры и искусств. - М. : МГУКИ, 2009. - 98 с. : ил. - Библиогр.: с. 98. - 5.

Дополнительная литература

1. Дрешер, Ю. Н. Организация информационного производства : учеб. пособие. - М. : Фаир-Пресс, 2005. - 245, [2] с.

9. Материально-техническое и программное обеспечение дисциплины (модуля)

Освоение дисциплины предполагает использование академической аудитории для проведения лекционных и семинарских занятий с необходимыми техническими средствами (телевизор, DVD), компьютерный класс с доступом к Интернету.

Документ составлен в соответствии с требованиями ФГОС ВО с учетом рекомендаций ПрООП ВО по направлению подготовки «Документоведение и архивоведение».

Автор - составитель – **Алексеев А.Ю.**, доцент кафедры информатизации культуры и электронных библиотек МГИК, кандидат философских наук.

Рецензент – **Делицин Л.Л.**, доктор технических наук.

Министерство культуры Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный институт культуры»

Социально-гуманитарный факультет
Кафедра документоведения и архивоведения

УТВЕРЖДАЮ
Декан факультета СГФ
_____К.В. Ивина
«26» октября 2015 г.

УТВЕРЖДАЮ
Зав. кафедрой документоведения и архивоведения
_____О.Н. Кокойкина
«28» сентября 2015 г.

Фонд оценочных средств

по дисциплине

Информационная безопасность и защита информации

Направление подготовки «Документоведение и архивоведение»

Москва - 2015

Перечень компетенций, формируемых при освоении дисциплины

Информационная безопасность и защита информации

ОК-10 - способность к использованию основных методов, способов и средств получения, хранения, переработки информации.

ОПК-6 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

ПК-17 - владение методами защиты информации.

Виды контроля по периодам обучения

Материалы для проведения текущего контроля:

Контрольные работы

Контрольная работа № 1. Работа с антивирусными программами.

Проверить на вирусы зараженный файл антивирусными программами (Касперского, Avast, DrWeb и др.) и сравнить результаты тестирования.

Контрольная работа № 2. Администрирование средств операционной системы.

Стандартными средствами Windows 10 осуществить разграничение доступа к файлам и устройствам общего и ограниченного доступа.

Контрольная работа № 3. Защита реляционной базы данных: проверка навыков разграничения доступа к базовым программных средствам на примере средств MS ACCESS.

Задание: Определить ключи отношений и задать оптимальный ключ для организации защиты информации в реляционной схеме:

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Группа:
ФИО:
Найти ключи отношения Ключи:

0 00

0 00

0 00

0 00

0 00

0 00

Контрольная работа № 4. Основы криптографии.

Закодировать свою фамилию, имя, отчество следующими методами:

1. Методом замены: простым и усложненным;
2. Методом перестановки: простым и усложненным;
3. Методом ключа.

Осуществить раскодирование информации. Сравнить результат.

Тест

1. Случайные угрозы информации.

Сбои
Отказы
Ошибки
Злоумышленные действия людей
Стихийные бедствия
Побочные влияния

2. Преднамеренные угрозы информации.

Сбои
Отказы
Ошибки
Злоумышленные действия людей
Стихийные бедствия
Побочные влияния

3.Угрозы физической целостности информации
Несанкционированная модификация
Присвоение чужого права
Несанкционированное получение
Искажение структуры
Уничтожение (искажение)

4.Угрозы логической структуры информации
Несанкционированная модификация
Присвоение чужого права
Несанкционированное получение
Искажение структуры
Уничтожение (искажение)

5. Угрозы конфиденциальности информации
Несанкционированная модификация
Присвоение чужого права
Несанкционированное получение
Искажение структуры
Уничтожение (искажение)

6.Угрозы права собственности информации
Несанкционированная модификация
Присвоение чужого права
Несанкционированное получение
Искажение структуры
Уничтожение (искажение)

7. Субъективные предпосылки появления угроз информации.
Недобросовестные сотрудники
Качественная недостаточность элементов системы
Разведорганы иностранных государств
Уголовные элементы
Количественная недостаточность элементов системы
Промышленный шпионаж

8. Технические устройства как источники угроз информации
Регистрация, передача, хранение, переработка, выдача
Общего назначения, прикладные, вспомогательные
Состояние атмосферы, побочные шумы, побочные сигналы
Посторонние лица, пользователи, персонал
Ручные, интерактивные, внутримашинные, сетевые

9. Модели, алгоритмы, программы как источники угроз информации

Регистрация, передача, хранение, переработка, выдача
Общего назначения, прикладные, вспомогательные
Состояние атмосферы, побочные шумы, побочные сигналы
Посторонние лица, пользователи, персонал
Ручные, интерактивные, внутримашинные, сетевые

10. Внешняя среда как источник угроз информации
Регистрация, передача, хранение, переработка, выдача
Общего назначения, прикладные, вспомогательные
Состояние атмосферы, побочные шумы, побочные сигналы
Посторонние лица, пользователи, персонал
Ручные, интерактивные, внутримашинные, сетевые

11.Компьютерные вирусы это программы,
обладающие способностью к саморазмножению, но для размножения им необходим носитель информации.
которые злоумышленно вводятся в состав программного обеспечения и в процессе обработки информации осуществляют несанкционированные процедуры.
обладающие способностью к саморазмножению, для размножения им не требуется носитель информации.
которые генерируются операционной системой в процессе старения информации.

12.”Троянские кони” это программы,
обладающие способностью к саморазмножению, но для размножения им необходим носитель информации.
которые злоумышленно вводятся в состав программного обеспечения и в процессе обработки информации осуществляют несанкционированные процедуры.
обладающие способностью к саморазмножению, для размножения им не требуется носитель информации.
которые генерируются операционной системой в процессе старения информации.

13.Компьютерные черви это программы,
обладающие способностью к саморазмножению, но для размножения им необходим носитель информации.
которые злоумышленно вводятся в состав программного обеспечения и в процессе обработки информации осуществляют несанкционированные процедуры.
обладающие способностью к саморазмножению, для размножения им не требуется носитель информации.
которые генерируются операционной системой в процессе старения информации.

14. Ожидаемая полная стоимость C;
Стоимость защиты Z;
Стоимость ущерба U;
Стоимость оптимальная O

15. Общедоступная информация
Определяет пользователь, устанавливающий степень защищенности.
Составляется список лиц, имеющих право доступа с указанием дней и времени доступа, а также перечня разрешенных процедур.
Не требуется специальных мер защиты от несанкционированного доступа.
Пользователи каждого структурного подразделения имеют право доступа только к “своим” данным.
Обеспечен свободный доступ пользователям учреждения-владельца.

16. Конфиденциальная информация
Определяет пользователь, устанавливающий степень защищенности.
Составляется список лиц, имеющих право доступа с указанием дней и времени доступа, а также перечня разрешенных процедур.
Не требуется специальных мер защиты от несанкционированного доступа.
Пользователи каждого структурного подразделения имеют право доступа только к “своим” данным.
Обеспечен свободный доступ пользователям учреждения-владельца

17. В стандарте США “Критерии оценки гарантированно защищенных вычислительных систем в интересах министерства обороны США” требования разделены на три группы:
Маркировка
Гарантии
Идентификация
Стратегия
Подотчетность

18. В документе Гостехкомиссии России «Классификация автоматизированных систем и требования по защите информации» ко второй группе относятся системы:
в которых работает один пользователь, допущенный ко всей обрабатываемой информации.
многопользовательские, в которых одновременно обрабатывается информация разных уровней конфиденциальности, различные пользователи имеют различные права на доступ к информации.
в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации.

многопользовательские, в которых работает один пользователь, допущенный ко всей обрабатываемой информации.

многопользовательские в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации.

19. Формальные способы обеспечения защиты информации:

Физические.

Морально-этические.

Законодательные.

Аппаратные.

Организационные.

Программные.

19. Программные средства обеспечения защиты информации:

Специальные пакеты программ или отдельные программы, предназначенные для решения задач защиты информации.

Сложившиеся в обществе нормы или правила, нарушение которых приравнивается к несоблюдению правил поведения.

Механические, электрические, электронные и т. п. устройства и системы, которые создают препятствия на пути дестабилизирующих факторов.

Мероприятия, специально предусматриваемые в технологии функционирования автоматизированных систем с целью решения задач защиты информации.

Различные механические, электронные и т. п. устройства, схемно встраиваемые в аппаратуру с целью решения задач защиты информации.

Нормативно-правовые акты, с помощью которых регламентируются права, обязанности и ответственность лиц, имеющих отношение к функционированию системы.

20. Внешняя защита, осуществляемая техническими средствами:

Охрана территории и помещений.

Подавление электромагнитного излучения.

Наблюдение.

Идентификация.

Разграничение доступа.

Блокировка

21.Технические требования к системе защиты информации:

Минимизация затрат на систему. Максимальное использование серийных средств

Структурированность всех компонентов системы. Простота эксплуатации.

Обеспечение решения требуемой совокупности задач защиты. Удовлетворение всем требованиям защиты.

Комплексное использование средств. Оптимизация архитектуры.

22. Программное обеспечение средств защиты информации

Совокупность методов, моделей и алгоритмов, необходимых для оценок уровня защищенности информации и решения других задач защиты.

Совокупность систем классификации и кодирования данных о защите информации, массивы данных средств защиты информации, а также входные и выходные документы средств защиты информации.

Совокупность языковых средств, необходимых для обеспечения взаимодействия компонентов средств защиты информации между собой, с компонентами автоматизированной системы и с внешней средой.

Совокупность программ, необходимых для решения задач управления механизмами защиты.

Совокупность средств, необходимых для поддержки решения всех задач защиты информации в процессе функционирования средств защиты информации.

23. Требуемый уровень и затраты на защиту для информации составляющей промышленную, коммерческую или банковскую тайну:

Зависит от важности научного направления и значимости полученных результатов. Затраты должны обеспечить требуемый уровень защиты.

Определяется размером выделяемых на защиту затрат. Затраты не должны превышать возможных потерь от преодоления защиты злоумышленником.

Высокий. Затраты должны обеспечить требуемый уровень защиты.

Определяется размером выделяемых на защиту затрат. Затраты определяются владельцем защищаемой информации.

24.Опознавание пользователя с помощью блоков-приставок заключается в

оснащении технических средств специальными устройствами, генерирующими индивидуальные сигналы.

изготовлении специальных карточек, на которые наносят специальный шифр, код и т.п.

создании записей, содержащие персонифицирующие пользователя данные. При обращении система предлагает назвать некоторые данные, которые затем сравниваются с хранящимися.

использовании отпечатков пальцев, геометрии рук, голоса, персональной росписи, структуры сетчатки глаза и др.

выдаче каждому пользователю персонального идентификатора, который он должен держать в тайне и вводить в ЭВМ при каждом обращении к ней.

25. Способы преобразования при шифровании.

Замена (подстановка).

Смысловое преобразование.
Перестановка.
Аналитическое преобразование.
Гаммирование.
Символьное преобразование.

26. Свойство информации при ее обработке техническими средствами, обеспечивающее предотвращение несанкционированного ознакомления с ней или снятия копий

Безопасность.
Секретность (конфиденциальность).
Целостность.
Доступность.
Угроза безопасности.

Материалы для проведения аттестации

5-й семестр.

1. Вид аттестации – зачет.
2. Форма проведения – устный опрос.

Перечень вопросов, выносимых на аттестацию

1. Понятия «информационная безопасность» и «защита информации».
2. Причины важнейшей роли информационной безопасности по сравнению с другими составляющими интегральной безопасности предприятия.
3. Основные источники угроз информационной безопасности.
4. Пассивные и активные способы реализации угроз безопасности информации.
5. Типы угроз безопасности информации.
6. Причины угроз безопасности информации.
7. Основные задачи, решение которых необходимо для защиты от НСД.
8. Классификация компьютерных преступлений.
9. Три наиболее опасные угрозы информационным системам.
10. Какой процент утечки коммерческой информации по оценке западных специалистов может привести к банкротству фирмы?
11. Основные способы перехвата и утечки информации.
12. Основные уровни обеспечения информационной безопасности.

13. Категории (грани) информации, подлежащие защите.
14. Базовые законодательные акты в области информационной безопасности.
15. Ключевые источники законодательных и нормативно-технических актов в области информационной безопасности.
16. Национальные интересы Российской Федерации в сфере информационной безопасности.
17. Основные источники государственных информационных ресурсов.
18. Виды и источники угроз национальной безопасности РФ.
19. Базовые мероприятия по обеспечению информационной безопасности РФ в сфере науки и техники.
20. Ключевые мероприятия по обеспечению информационной безопасности РФ в информационных и телекоммуникационных системах.
21. Основные составляющие руководящего документа, характеризующие политику безопасности организации.
22. Административный уровень защиты: анализ рисков для информационной системы организации.
23. Этапы работ по обеспечению информационной безопасности на административном уровне.
24. Стандарты в области разработки политики безопасности и анализа рисков.
25. Группы процедурных мер для обеспечения информационной безопасности.
26. Физические средства защиты информации.
27. Ключевые направления поддержания работоспособности компьютерных систем.
28. Основные функции программных средств по обеспечению информационной безопасности.
29. Классификация сервисов программных средств защиты информации.
30. Идентификация и аутентификация – основа программно-технических средств обеспечения безопасности.
31. Основные мероприятия по повышению надежности парольной защиты.

6-й семестр.

1. Вид аттестации – экзамен.
2. Форма проведения – устный опрос.

Перечень вопросов, выносимых на аттестацию.

1. Антивирусные программные продукты.
2. Базовые организационные меры безопасности для предотвращения «вирусных» атак.
3. Криптографические средства защиты информации.
4. Различия в криптографическом и стеганографическом методах защиты информации.
5. Классы и группы защищенности средств вычислительной техники от несанкционированного доступа к информации.
6. Классификация информационных систем в РФ по уровню безопасности.
7. Основные принципы обеспечения архитектурной безопасности информационных систем.
8. Стандарты в области безопасности распределенных систем.
9. Базовые сервисы обеспечения безопасности для информационных систем.
10. Виды деятельности в области защиты информации, подлежащие лицензированию Гостехкомиссией России.
11. Основные способы реагирования на нарушения информационной безопасности.
12. Классификация сбоев и нарушений в сетях передачи информации.
13. Основные средства защиты информации в сети:
14. Система Kerberos как пример комплексного решения контроля доступа в сети.
15. Этапы организации разграничения доступа к информации в сети.
16. Основные задачи, решаемые при создании механизмов разграничения доступа к информации.
17. Базовая схема защиты и обеспечения информации К.Шеннона
18. Криптографические методы защиты информации
19. История развития криптографии.
20. Базовые методы криптографической защиты.
21. Специфика криптографии в условиях электронного документооборота.
22. Алгоритмы криптографической защиты методом перестановок, замены и ключа.
23. Стандарт RSA
24. Стандарт DES
25. Стандарт AES
26. Алгоритмы криптографической защиты методом замены
27. Концептуальная схема деятельности по обеспечению

безопасности и защиты информации.

28. Модель офицера ОБИ.
29. Алгоритмы криптографической защиты методом ключа
30. Угрозы информационной безопасности в компьютерных системах
31. Классификация угроз информационной безопасности.
32. Специфика угроз в компьютерных технологиях информационных систем.
33. Стандарт криптографической защиты данных DES
34. Программы защиты информации программных средств общего назначения.
35. Программы защиты информации базовых программных средств.
36. Многообразие программ защиты информации специального назначения.
37. Концептуальная схема утечки информации по техническим каналам. Параметры утечки.
38. Общая характеристика средств защиты информации от утечки по техническим каналам.
39. Поточные шифры
40. Защита информации от несанкционированного доступа
41. Общая характеристика средств защиты о НСД в общих, базовых и специальных программных средствах.
42. Понятие ядра защиту операционной системы.
43. Классификация диверсионных программных средств: троянские кони, вирусы, черви.
44. Модель распространения и заращения компьютерного вируса. Основные угрозы от вирусных атак.
45. Примеры программ – вирусов.
46. Алгоритмы шифрования с открытым ключом
47. Алгоритмы цифровой подписи
48. Концептуальная схема защиты информации в документообороте.
49. Роль генераторов псевдослучайных последовательностей в обеспечении защиты информации
50. Понятия конфиденциальных документов.
51. Концептуальная схема защиты информации во входном потоке документов.
52. Классификация и структуризация входных документов. Защита иерархически структурированной информации.
53. Преимущество фасетной классификации документов.
54. Концептуальные схемы зашиты информации в сетевых, иерархических и реляционных моделях хранения данных.

55. Проблема рекламы и обеспечение безопасности информации.
56. Электронные цифровые подписию
57. Принципы и условия использования электронной цифровой подписи.
58. Использование электронной цифровой подписи в сфере организационного управления.

Помимо этих вопросов, на экзамен выносится один из вопросов аттестации первого семестра (см. выше).

Критерии и показатели оценивания результатов обучения

Планируемые результаты обучения по дисциплине

Результаты освоения образовательной программы *(код и формулировка компетенций)*	**Уровень освоения компетенции**	**Перечень планируемых результатов обучения по дисциплине** *(в целях формирования названной компетенции)*
способностью к использованию основных методов, способов и средств получения, хранения, переработки информации (ОК-10)	базовый	**знать:** • базовые понятия об информации и информационных технологиях; • предмет и основные способы организации информационных технологий, автоматизированных информационных технологий; • эволюцию и перспективы развития информационных технологий, их роль в технологизации социального пространства; • основы технологий, связанных с обработкой и представлением информации;

		• классификацию информационных технологий; • правила построения, варианты оформления и эффективность построения различных схем и технологических процессов в информационных системах; • методику построения индивидуальных информационных технологий и специфику создания интерфейса пользователя; • интеграцию разных видов и классов информационных технологий в реализации информационных процессов.
		уметь: • выделять элементы технологических процессов из текстового описания регламента процесса; • представлять технологические процессы обработки информации в удобной для восприятия форме; • пользоваться стандартными методами расчета характеристик технологических процессов; • строить диаграммы Ганта для информационно-технологических процессов; • документировать функциональные характеристики будущего программного продукта, входные данные и результирующую информацию,

		• иметь представление: • об истории появления и развития информационных технологий; • о типовых технологических процессах обработки информации; • о технологических процессах управления в системах;
		владеть: • навыками анализа и построения технологических процессов обработки данных в реализации прикладных информационных процессов; • способами построения графических пользовательских интерфейсов, разработки форм и основных элементов управления; • навыками документирования процесса эксплуатации программного изделия.
Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-6);	базовый	**Знать** основные понятия, виды, свойства измерения и кодирования информации; знать эволюцию информационных технологий и их роль в развитии общества; **владеть** методами и средствами защиты информации; дать характеристику процессам сбора, хранения и передачи информации; классифицировать носители информации; **знать** стандарты государственных требований о защите информации; обеспечивать защиту информации в соответствии с государственными требованиями.

Владение методами защиты информации (ПК-17)	базовый	**Знать** сущность и принципы экономической безопасности предпринимательской деятельности, концепцию информационной безопасности, правовые аспекты безопасности информационных ресурсов, основные направления и методы функционирования систем защиты информации. **Уметь** использовать различные типы технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов, использовать методы работы с персоналом, обладающим конфиденциальной информацией, методику защиты информации при проведении деловых мероприятий. Осуществлять организацию функционирования систем защиты информации, служб безопасности, конфиденциального документооборота.

Критерии и показатели оценки

Критерии	**Оценка**			
	Зачет (Отлично)	**Зачет (Хорошо)**	**Зачет (Удовлетвори-тельно)**	**Незачет (Неудовлетво-рительно)**
1. Знание теоретических основ	Студент демонстрирует глубокое знание теоретических основ, базовых понятий и категорий дисциплины	Студент хорошо владеет знаниями теоретических основ, базовыми понятиями и категориями дисциплины	Студент затрудняется с изложением теории, поверхностно ориентируется в базовых понятиях и категориях дисциплины	Студент не понимает проблемы, механически повторяет некоторые положения теории, не разбирается в базовых понятиях и

				категориях дисциплины
2. Умение применять теоретические знания при решении практических задач	Студент свободно реализует теоретические положения при выполнении практического задания	Студент испытывает некоторые затруднения и / или допускает неточности при выполнении практического задания	Студент выполняет практическое задание после наводящих вопросов, допускает при этом ошибки	Студент демонстрирует неумение применять теоретические знания для решения практических задач
3. Владение профессиональной термино-логией	Студент демонстрирует свободное владение понятийным аппаратом дисциплины	Студент хорошо владеет профессиональной терминологией, в случае ошибки в употреблении термина способен самостоятельно исправить ее	Студент слабо владеет профессиональной терминологией, допускает ошибки в интерпретации терминов	Студент не владеет профессиональ-ной термино-логией
4. Аргумен-тация	Студент использует различные операции логического вывода: анализ, синтез, обобщение, сравнение и др. Свободно выстраивает аргументацию	Студент предъявляет достаточно стройный, лаконичный и четкий ответ, но допускает незначительное количество ошибок при аргументировании своей позиции	Студент нарушает логику изложения, демонстрирует недостаточную аргументацию	Студент допускает грубые ошибки в логическом выводе, не может аргументиро-вать свою позицию
5. Характер реализации навыков устной речи	Студент демонстрирует высокую культуру речи	Речь грамотна и стилистически корректна, но содержит отдельные неточности	В речи встречаются нарушения норм литературного языка	Речь студента фрагментарна, изобилует паузами и нарушениями норм литературного языка

Критерии оценки знаний студентов при проведении опроса:

- оценка «отлично» выставляется студенту за активное участие в обсуждении всех вопросов темы занятия и за содержательный ответ на один из вопросов;

- оценка «хорошо» - содержательный ответ по одному из вопросов тем семинара;

- оценка «удовлетворительно» - неполное сообщение по вопросу темы и неубедительный ответ на вопросы преподавателя;

- оценка «неудовлетворительно» - незнание ответа на вопросы преподавателя по теме занятия.

Критерии оценки выполненной студентом контрольной работы:

Контрольная работа должна быть:

- выполнена по заданию педагога и в соответствии с условиями работы;

- реализована самостоятельно;

- оформлена с соблюдением всех требований, предъявляемых к оформлению контрольной работы.

Оценка «отлично» выставляется студенту, если он уверенно и в полном объеме выполнил предложенное преподавателем задание.

Оценка «хорошо» выставляется студенту, если он уверенно и в полном объеме выполнил предложенное преподавателем задание, имеется несколько незначительных ошибок.

Оценка «удовлетворительно» выставляется студенту, если он неуверенно и не в полном объеме выполнил предложенное преподавателем задание.

Оценка «неудовлетворительно» выставляется студенту, если он не выполнил предложенное преподавателем задание.

Критерии оценки выполнения студентом тестирования

Оценка «отлично» выставляется студенту, если он правильно ответил на 85-100 % вопросов теста.

Оценка «хорошо» выставляется студенту, если он правильно ответил на 70-84 % вопросов теста.

Оценка «удовлетворительно» выставляется студенту, если он правильно ответил на 55-69 % вопросов теста.

Оценка «неудовлетворительно» выставляется студенту, если он правильно ответил менее, чем на 55% вопросов теста.

Порядок выставления общей оценки в рамках аттестации

Аттестация по дисциплине в 5 семестре проходит **в форме зачета, в 6 семестре – в форме экзамена**

и отражает комплексный характер учета работы студента по параметрам:

- посещаемости занятий;

- количества сообщений по проблематике семинаров;

- активности работы на семинарских занятиях;
- оценки докладов и презентаций;
- оценки качества выполненных практических заданий по дисциплине;
- оценки контрольных работ;
- оценки ответа на зачете.

Критерии оценки

Зачет (оценка «отлично») соответствует:

- не менее 90% посещаемости занятий;
- не менее двух выступлений по тематике семинаров;
- активное участие в обсуждении вопросов семинарских занятий;
- своевременное представление и качественная подготовка докладов и презентаций;
- положительные оценки выполнения практических работ;
- положительные оценки контрольных работ;
- полное знание вопросов при ответе на зачете.

Зачет (оценка «хорошо») соответствует:

- не менее 80% посещаемости занятий;
- не менее одного выступления по тематике семинаров;
- участие в обсуждении вопросов семинарских занятий;
- своевременное представление и качественная подготовка докладов и презентаций;
- положительные оценки выполнения практических работ;
- положительные оценки контрольных работ;
- хорошее знание вопросов при ответе на зачете.

Зачет (оценка «удовлетворительно») соответствует:

- не менее 70% посещаемости занятий;
- не менее одного выступления по тематике семинаров;
- представление и подготовка докладов и презентаций;
- положительные оценки выполнения практических работ;
- положительные оценки контрольных работ;
- удовлетворительное знание вопросов при ответе на зачете.

Незачет (оценка «неудовлетворительно») соответствует:

- пропуски более 50% занятий без уважительных причин;
- отсутствие выступлений по темам семинаров;
- пассивность при обсуждении вопросов семинаров;
- наличие отрицательных оценок выполнения практических работ;
- наличие отрицательных оценок контрольных работ;
- неудовлетворительное знание вопросов при ответе на зачете.

Документ составлен в соответствии с требованиями ФГОС ВО с учетом рекомендаций ПрООП ВО по направлению подготовки «Документоведение и архивоведение».

Автор - составитель – **Алексеев А.Ю.**, доцент кафедры информатизации культуры и электронных библиотек МГИК, кандидат философских наук.

Рецензент – **Делицин Л.Л.**, доктор технических наук.

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Московский государственный институт культуры»

УТВЕРЖДАЮ
Декан факультета СГФ
_____К.В. Ивина
«26» октября 2015 г.

УТВЕРЖДАЮ
Зав. кафедрой
документоведения и
архивоведения
_____О.Н.
Кокойкина
«28» сентября 2015 г.

Методические указания
для проведения семинарских и практических занятий
по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки

Документоведение и архивоведение

Профиль подготовки

Документоведение и документационное обеспечение управления

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная, заочная

Согласовано:

С председателем методического совета по качеству по направлению «Документоведение и архивоведение» О.Н. Кокойкиной_____

Москва - 2015

1. Методические указания для студентов общего характера

Изучение учебного материала целесообразно посредством оптимального сочетания аудиторных занятий (лекции, тематические семинарские и практические занятия) и самостоятельной работы студентов (изучение материалов лекций и и литературы, самостоятельная отработка практических навыков на основе выполненных практикумов, подготовка к опросам, тестам, контрольным работам, зачету и экзамену).

Основными **видами учебных занятий** по дисциплине «Информационная безопасность и защита информации» являются лекции и практические работы.

Лекции имеют целью дать стройную систему научных знаний по дисциплине; сформировать у студентов научный подход к организации информационных систем и технологий; обеспечить понимание состава и функций основных и специализированных информационных технологий; показать многообразие подходов к проектированию и организации документооборота; дать методические основы, принципы и технологические основы ведения и поддержки информационных средств документооборота.

Важное место в процессе изучения дисциплины занимают *практические занятия.* Эти занятия предназначены для углубления и закрепления знаний, полученных обучаемыми в ходе лекций и самостоятельной работы; просмотра источников различной информации; формирования у обучаемых навыков самостоятельного анализа информационных ресурсов по теме; отработке практических навыков работы с различными видами информационных технологий и применения их в практической деятельности. .

Значимую роль в подготовке играет *самостоятельная работа* обучаемых. Она имеет целью закрепление и расширение полученных в ходе лекционных занятий знаний; приобретение новых знаний; обобщение, систематизацию и практическое применение знаний; формирование практических умений и навыков; самоконтроль в процессе усвоения знаний; подготовку к предстоящим занятиям.

Задача преподавателя в рамках самостоятельной работы студентов заключается в том, чтобы максимально обеспечить условия для самостоятельного получения знаний из различных источников (публикации в отраслевой печати, материалы web-сайтов библиотек и научно-информационных учреждений, полнотекстовые базы и электронные библиотеки). Списки основной и дополнительной литературы и интернет-ресурсов по курсу представлены в Рабочей программе дисциплины.

2. Методические указания по подготовке к мероприятиям текущего контроля и аттестации

Важной частью дидактической системы по дисциплине «Информационная безопасность и защита информации» являются вопросы организации текущего контроля и аттестации.

Текущий контроль знаний служит для выявления степени усвоения учебного материала по изучаемой дисциплине. Он должен осуществляться в пределах всех организационных форм обучения, тщательно планироваться и призван выявить объем, глубину и качество восприятия изучаемого материала, определить имеющиеся пробелы в знаниях, наметить пути их устранения; выявить уровень овладения навыками самостоятельной работы; стимулировать интерес студентов к дисциплине. На практических занятиях текущий контроль теоретических знаний осуществляется, как правило, в форме опроса, тестирования. Также предусмотрены контрольные работы, которые студент выполняет в ходе самостоятельной подготовки.

Критерии оценки знаний студентов при проведении опроса:

- оценка «отлично» выставляется студенту за активное участие в обсуждении всех вопросов темы занятия и за содержательный ответ на один из вопросов;

- оценка «хорошо» - содержательный ответ по одному из вопросов тем семинара;

- оценка «удовлетворительно» - неполное сообщение по вопросу темы и неубедительный ответ на вопросы преподавателя;

- оценка «неудовлетворительно» - незнание ответа на вопросы преподавателя по теме занятия.

Критерии оценки выполненной студентом контрольной работы:

Контрольная работа должна быть:

- выполнена по заданию педагога и в соответствии с условиями работы;

- реализована самостоятельно;

- оформлена с соблюдением всех требований, предъявляемых к оформлению контрольной работы.

Оценка «отлично» выставляется студенту, если он уверенно и в полном объеме выполнил предложенное преподавателем задание.

Оценка «хорошо» выставляется студенту, если он уверенно и в полном объеме выполнил предложенное преподавателем задание, имеется несколько незначительных ошибок.

Оценка «удовлетворительно» выставляется студенту, если он неуверенно и не в полном объеме выполнил предложенное преподавателем задание.

Оценка «неудовлетворительно» выставляется студенту, если он не выполнил предложенное преподавателем задание.

Критерии оценки выполнения студентом тестирования

Оценка «отлично» выставляется студенту, если он правильно ответил на 85-100 % вопросов теста.

Оценка «хорошо» выставляется студенту, если он правильно ответил на 70-84 % вопросов теста.

Оценка «удовлетворительно» выставляется студенту, если он правильно ответил на 55-69 % вопросов теста.

Оценка «неудовлетворительно» выставляется студенту, если он правильно ответил менее, чем на 55% вопросов теста.

Аттестация по дисциплине проводится в 5 семестре в форме зачета в 6 семестре в форме экзамена и отражает комплексный характер учета работы студента по параметрам:

- посещаемости занятий;
- количества сообщений по проблематике семинаров;
- активности работы на семинарских занятиях;
- оценки докладов и презентаций;
- оценки качества выполненных практических заданий по дисциплине;
- оценки контрольных работ.

Перечень вопросов к зачету, охватывающий весь материал дисциплины, представлен в Фонде оценочных средств по дисциплине.

Критерии оценки

Зачет (оценка «отлично») соответствует:

- не менее 90% посещаемости занятий;
- не менее двух выступлений по тематике семинаров;
- активное участие в обсуждении вопросов семинарских занятий;
- своевременное представление и качественная подготовка докладов и презентаций;
- положительные оценки выполнения практических работ;
- положительные оценки контрольных работ;
- полное знание вопросов при ответе на зачете.

Зачет (оценка «хорошо») соответствует:

- не менее 80% посещаемости занятий;
- не менее одного выступления по тематике семинаров;
- участие в обсуждении вопросов семинарских занятий;
- своевременное представление и качественная подготовка докладов и презентаций;
- положительные оценки выполнения практических работ;
- положительные оценки контрольных работ;
- хорошее знание вопросов при ответе на зачете.

Зачет (оценка «удовлетворительно») соответствует:

- не менее 70% посещаемости занятий;
- не менее одного выступления по тематике семинаров;
- представление и подготовка докладов и презентаций;
- положительные оценки выполнения практических работ;
- положительные оценки контрольных работ;
- удовлетворительное знание вопросов при ответе на зачете.

Незачет (оценка «неудовлетворительно») соответствует:

- пропуски более 50% занятий без уважительных причин;
- отсутствие выступлений по темам семинаров;
- пассивность при обсуждении вопросов семинаров;
- наличие отрицательных оценок выполнения практических работ;
- наличие отрицательных оценок контрольных работ;
- неудовлетворительное знание вопросов при ответе на зачете.

3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Помимо рекомендованных в Рабочей программе дисциплины основной и дополнительной литературы, интернет-ресурсов, в процессе самостоятельной работы студенты могут пользоваться актуальными публикациями в отечественных и зарубежных профильных периодических изданиях (среди которых журналы «Научные и технические библиотеки», «Научно-техническая информация. Сер. 2. Информационные процессы и системы), а также раздаточными материалами, предлагаемыми педагогом.

4. Перечень информационных технологий, рекомендуемых при осуществлении образовательного процесса по дисциплине

При чтении лекций по всем темам целесообразно активно использовать компьютерную технику для демонстрации слайдов с помощью программного приложения Microsoft Power Point. На семинарских и практических занятиях студенты могут представлять презентации, подготовленные ими с помощью программного приложения Microsoft Power Point в часы самостоятельной работы.

Информационные технологии:

- сбор, хранение, систематизация и выдача учебной и научной информации;
- обработка текстовой, графической и эмпирической информации;
- подготовка, конструирование и презентация итогов учебно-исследовательской и аналитической деятельности;
- самостоятельный поиск дополнительного учебного и научного материала с использованием поисковых систем и сайтов сети Интернет, электронных энциклопедий и баз данных;
- использование электронной почты преподавателей и студентов для рассылки, переписки и обсуждения возникших учебных проблем.

***Программное обеспечение*:**

- операционная система класса Microsoft Windows XP или аналогичная;
- Microsoft Office версии 2003/2007/2010;
- браузеры Internet Explorer, Mozilla Firefox, Google Chrome, Opera;
- информационно-поисковые системы сети Интернет, в том числе Yandex, Google, Yahoo, Rambler и др.;
- Среда разработки Visual Studio.

Все методические усилия преподавателя по организации самостоятельной работы должны быть направлены на то, чтобы научить студентов самостоятельно мыслить, творчески усваивать изучаемый материал, анализировать и интерпретировать данные, показатели, понятия и идеи, работать с рекомендованными литературными источниками, в т.ч. периодическими изданиями, находить необходимую информацию и использовать её в учебно-научных целях.

Составитель: кандидат философских наук, А.Ю. Алексеев.