Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ИНСТИТУТ ОТРАСЛЕВОГО МЕНЕДЖМЕНТА

Факультет маркетинга, рекламы и сервиса
Кафедра рекламы и связей с общественностью

УТВЕРЖДЕНА

решением кафедры Рекламы и связей с общественностью

Протокол от «___» _____201_ г.

№_____

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.2.2 Информационная безопасность

по направлению подготовки
42.03.01 – Реклама и связи с общественностью
Направленность (профиль) "Реклама и связи с общественностью в коммерческой сфере"

Квалификация
Бакалавр

Форма обучения
Очная

Год набора – 2017

Москва, 2017 г.

Автор-составитель:

Старший преподаватель А.В.Иванов

Заведующий Кафедрой рекламы и связей с общественностью,

д.филол.н., профессор В.А.Евстафьев

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

2. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся и место дисциплины в структуре образовательной программы

3. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий и структура дисциплины

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

5. Методические указания для обучающихся по освоению дисциплины

6. Основная и дополнительная учебная литература, необходимая для освоения дисциплины (модуля), ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

7. Материально-техническая база, информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.В.ДВ.2.12 «Информационная безопасность» обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-5	Способность реализовывать проекты и владение методами их реализации.	ПК-5.1	Способность к свободному владению навыками реализации творческих проектов посредством компьютерных графических программ, а также освоение методов реализации рекламных проектов с использованием профессиональных компьютерных технологий, построения математических моделей и оптимизации бизнес-процессов

1.2. В результате освоения дисциплины Б1.В.ДВ.2.12 «Информационная безопасность»у студентов должны быть сформированы:

ОТФ/ТФ	Код этапа освоения компетенции	Результаты обучения
ПС-11.005 А Творческо-организационная деятельность по созданию новых продуктов телерадиовещательных СМИ А/01.6 - определение формата, тематики и оценка материала для нового продукта телерадиовещательных СМИ; А/02.6 - подготовка создания сценарного материала нового продукта; А/03.6 - планирование создания нового продукта телерадиовещательных СМИ; А/05.6 - организация обеспечения производственного процесса создания нового продукта телерадиовещательных СМИ	ПК-5.1	**на уровне знаний:** классификация угроз по информационным ресурсам; современные проблемы информационной безопасности; основные концептуальные положениями системы защиты информации; основные направления обеспечения информационной безопасности; **на уровне умений:** меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи; **на уровне навыков:** использование современных методов

необходимыми ресурсами; А/06.6 - организация деятельности рабочей группы по созданию нового продукта телерадиовещательных СМИ; А/07.6 - организация продвижения готовых продуктов и продуктов на этапе создания		защиты информации в компьютерных системах; осуществление мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными.

2. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся и место дисциплины в структуре образовательной программы

Объем дисциплины

Вид учебных занятий и самостоятельная работа		**Всего**
Очная форма обучения		
Контактная работа обучающихся с преподавателем, в том числе:		***40***
лекционного типа (Л)		***10***
лабораторные работы (практикумы) (ЛР)		
практического (семинарского) типа (ПЗ)		***30***
Самостоятельная работа обучающихся (СР)		***32***
Промежуточная аттестация	**форма**	***Зачет***
	час.	
Общая трудоемкость (час. / з.е.)		***72/2***

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.2.2 «Информационная безопасность» осваивается в 4 семестре по очной форме, общая трудоемкость – 2 зачетные единицы.

Освоение дисциплины опирается на минимально необходимый объем теоретических знаний в области базовых экономических понятий (спрос, предложение, цена, стоимость, товар, деньги, доходы, расходы, прибыль, риск, собственность, управление, рынок, фирма, государство), объективных основ функционирования экономики и поведения экономических агентов (законы спроса и предложения, принципы ценообразования, принцип ограниченной рациональности, принцип альтернативных издержек, принцип изменения ценности денег во времени), особенностей экономических процессов в мировом экономическом пространстве, а также на приобретенные ранее умения и навыки использования понятийного аппарата экономической науки для описания экономических и финансовых процессов.

Дисциплина реализуется после изучения дисциплин: Б1.Б.13 «Компьютерные технологии и информатика» и является основой для изучения дисциплины Б1.В.ОД.5 Управление проектом и др.

Форма промежуточной аттестации – зачет.

3. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий и структура дисциплины

Структура дисциплины

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.					Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий			СР	
			Л	ЛР	ПЗ		
Очная форма обучения							
Раздел 1	Концепция информационной безопасности.	14	2		6	6	
Раздел 2	Угрозы информации.	14	2		6	6	Т
Раздел 3	Виды возможных нарушений информационной системы.	14	2		6	6	Т
Раздел 4	Информационная безопасность информационных систем.	14	2		6	6	Р
Раздел 5	Методы и средства защиты компьютерной информации.	16	2		6	8	Т
Промежуточная аттестация							зачет
Всего:		**72**	**10**		**30**	**32**	

**Примечание: формы текущего контроля успеваемости: тестирование (Т), реферат (Р).*

Содержание дисциплины

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Раздел 1	Концепция информационной безопасности.	Актуальность информационной безопасности. Актуальность информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Лицензирование и сертификация в области защиты информации. Законодательство в области лицензирования и

		сертификации. Правила функционирования системы лицензирования. Основные нормативные руководящие документы. Международные стандарты информационного обмена. Критерии безопасности компьютерных систем. «Оранжевая книга». Руководящие документы Гостехкомиссии.
Раздел 2	Угрозы информации.	Информационная безопасность сетей. Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ. Способы совершения компьютерных преступлений. Уязвимость сети Интернет. Пользователи и злоумышленники в Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.
Раздел 3	Виды возможных нарушений информационной системы	Компьютерные преступления. Классификация компьютерных преступлений. Виды противников или «нарушителей». Вредоносные программы. Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам. Вирусы. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.
Раздел 4	Информационная безопасность информационных систем.	Теория информационной безопасности информационных систем. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Криптографические способы защиты информации. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись. Организация информационной безопасности компании. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.
Раздел 5	Методы и средства защиты компьютерной информации.	Обеспечения информационной безопасности. Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Контроль доступа к информации. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта). Методы и средства защиты информации. Методы и

		средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Антивирусное ПО. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

4. Материалы текущего контроля успеваемости обучающегося и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

– при проведении занятий лекционного типа: объяснительно-иллюстративный метод с элементами проблемного изложения учебной информации (монологической, диалогической или эвристической);

– при проведении занятий семинарского типа: тесты, рефераты

4.1.2. Зачет проводится в виде практических заданий на компьютере

4.2. Материалы текущего контроля успеваемости

Текущая аттестация по дисциплине проводится в форме опроса и контрольных мероприятий по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

– учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

– степень усвоения теоретических знаний;

– уровень овладения практическими умениями и навыками по всем видам учебной работы;

– результаты самостоятельной работы.

Все задания, используемые для текущего контроля успеваемости, делятся на две группы:

1) задания, которые в силу своих особенностей могут быть реализованы только в процессе обучения (доклад, ролевая игра и т.п.);

2) задания, которые дополняют теоретические вопросы (практические задания, кейс).

Выполнение заданий первого типа является необходимым для формирования и контроля ряда умений и навыков. Поэтому, в случае невыполнения заданий в процессе обучения, их необходимо «отработать» до проведения промежуточной аттестации. Вид заданий, которые необходимо выполнить для ликвидации «задолженности» определяется в индивидуальном порядке, с учетом причин невыполнения.

Тест по дисциплине

1. Задание. В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

2. Задание. Сертификации подлежат:

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. все вышеперечисленные средства.

3. Задание. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

4. Задание.

Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

5. Задание. Хакер – это:

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;

3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;

4. плохой игрок в гольф, дилетант;

5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

6. Задание. Активный перехват информации - это перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

3. неправомерно использует технологические отходы информационного процесса;

4. осуществляется путем использования оптической техники;

5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

7. Задание. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;

2. фишинг;

3. нигерийские письма;

4. источник слухов;

5. пустые письма.

8. Задание. По среде обитания классические вирусы разделяются:

1. на паразитические;

2. на компаньоны;

3. на файловые;

4. на ссылки;

5. на перезаписывающие.

9. Задание. Шифрование методом подстановки:

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;

2. символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;

3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;

4. символы шифруемого текста заменяются другими символами, зятыми из одного или нескольких алфавитов;

5. замена слов и предложений исходной информации шифрованными.

10. Задание. Метод защиты информации ограничение доступа заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;

2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;

3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;

4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;

5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

11. Задание. Перехват, который неправомерно использует технологические отходы информационного процесса, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

12. Задание. Спам, периодически проводящий рассылки не рекламных сообщений:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

13. Задание. Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от …

1. среды распространения электромагнитного сигнала;
2. длины волны сигнала;
3. наличия или отсутствия специальной линии связи;
4. типа линии связи;
5. форм воздействия на информацию или ее носитель;
6. предполагаемого способа нападения на информацию.

14. Задание. Попытка одного субъекта выдать себя за другого - это:

1. пассивная атака;
2. модификация потока данных»;
3. фальсификация;
4. повторное использование;
5. отказ в обслуживании.

15. Задание. В качестве биометрических признаков, которые могут быть использованы при идентификации субъекта доступа, можно выделить:

1. должностное лицо;
2. терминал;
3. распечатка;
4. форма и размеры лица;

5. оператор.

16. Задание. Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

Примерная тематика рефератов

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
6. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
7. Информационная безопасность (по материалам зарубежных источников и литературы).
8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
12. Составление инструкции по обработке и хранению конфиденциальных документов.
13. Направления и методы защиты документов на бумажных носителях.
14. Направления и методы защиты машиночитаемых документов.
15. Архивное хранение конфиденциальных документов.
16. Направления и методы защиты аудио- и визуальных документов.
17. Порядок подбора персонала для работы с конфиденциальной информацией.
18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
23. Порядок защиты информации в рекламной и выставочной деятельности.
24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

28. Назначение, виды, структура и технология функционирования системы защиты информации.

29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

30. Аналитическая работа по выявлению каналов утечки информации фирмы.

31. Анализ функций персонала фирмы в области защиты информации.

32. Направления и методы защиты профессиональной тайны.

33. Направления и методы защиты служебной тайны.

34. Направления и методы защиты персональных данных о гражданах.

35. Методы защиты личной и семейной тайны.

36. Построение и функционирование защищенного документооборота.

37. Защита секретов в зарубежных рекламных агентствах.

38. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

4.3. Оценочные средства для промежуточной аттестации

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-5	Способность реализовывать проекты и владение методами их реализации.	ПК-5.1	Способность к свободному владению навыками реализации творческих проектов посредством компьютерных графических программ, а также освоение методов реализации рекламных проектов с использованием профессиональных компьютерных технологий, построения математических моделей и оптимизации бизнес-процессов

4.3.2. Показатели и критерии оценивания компетенций на различных этапах их формирования

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПК-5.1	Изучает: Представление цвета в компьютере. Графические файлы. Аппаратные средства компьютерной графики. Растровая графика. Алгоритмы растеризации. Основные приемы работы в растровом редакторе. Практическое применение растровой графики в рекламе. Векторная графика. Алгоритмы векторизации. Работа с графическим изображением. Основные приемы работы в векторном редакторе. Практическое применение векторной графики в рекламе. Структурирует информационные ресурсы в соответствии с их ценностью и полезностью, определению необходимости их защиты от несанкционированного доступа; определяет направления актуализации системы защиты информации в соответствии с текущими деловыми потребностями субъекта бизнеса и выявленным уровнем уязвимости защищаемой информации; анализирует уровень защищенности документов в процессе их движения, рассмотрения, использования и исполнения. Изучает: Прикладная эконометрика; современные инструментальные программные средства ПК для обработки данных, построения математических моделей и оптимизации бизнес-процессов; работа с реальной рыночной информацией и	Изучены: алгоритмические и математические основы построения моделей компьютерной графики; основные средства компьютерной графики; основы моделирования процессов создания рекламного продукта; основы векторной, растровой, фрактальной графики; алгоритмы построения рекламных продуктов с помощью компьютерной графики; Программно реализованы основные алгоритмы растровой и векторной графики; использованы графические стандарты и библиотеки; применены механизмы конструирования рекламы в соответствии с маркетинговыми целями организации; смоделированы и реализованы проекты графического построения рекламного образа путем компьютерной графики; Продемонстрировано владение основными приемами создания и редактирования изображений в векторных редакторах; ретуширования и подготовки к производству изображений в растровых редакторах; использованы инновационные возможности графических систем в области конструирования рекламы; продемонстрированы навыкипо рациональному применению компьютерных технологий построения и реализации рекламных продуктов. Использованы современные методы защиты информации в компьютерных системах; Осуществлены мероприятия по обеспечению информационной безопасности, функционированию информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными. Применены методы

	построение на ее основе эконометрических моделей; формализации реальных бизнес-процессов в виде математических моделей; решение задач оптимизации.	количественного анализа и моделирования, теоретического и экспериментального исследования; построены экономические, финансовые и организационно-управленческие модели с помощью инструментов и вычислительных средств; использованы технологии, инструменты и вычислительные средства при моделировании; проанализирована внутренняя и внешняя среда объекта менеджмента; проведена оценка эффективности результатов деятельности.

4.3.3 Типовые контрольные задания или иные материалы (типовые оценочные материалы), необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету по дисциплине

1. Необходимость защиты информации.
2. Сохранность защищаемой информации: сущность и основные виды. Сущность понятия "защищаемая информация".
3. Разновидность защищаемой информации и ее носителей.
4. Компьютерные вирусы и их классификация.
5. Характеристика антивирусного программного обеспечения.
6. Способы ограничение доступа к информации.
7. Предотвращение технических сбоев оборудования.
8. Методы взлома компьютерных систем. Атаки на уровне систем управления базами данных.
9. Методы взлома компьютерных систем. Атаки на уровне операционной системы.
10. Методы взлома компьютерных систем. Атаки на уровне сетевого программного обеспечения.
11. Методы взлома компьютерных систем. Защита системы от взлома.
12. Характеристика троянских программ. Возникновение троянских программ.
13. Характеристика троянских программ. Где и как часто встречаются троянские программы.
14. Характеристика троянских программ. Распознавание троянской программы.
15. Программные закладки и их классификация.
16. Модели воздействия программных закладок на компьютеры.
17. Защита системы от программных закладок.
18. Разновидность ПЗ (имитаторы, фильтры и заместители).

19. Парольные взломщики. Защита системы от клавиатурных шпионов. Парольная защита операционных систем.

20. Взлом парольной защиты ОС UNIX.

21. Взлом парольной защиты ОС Windows NT.

22. Информационная безопасность компьютерной сети. Характеристика и назначение сканеров.

23. Информационная безопасность компьютерной сети. Характеристика и назначение анализаторов протоколов.

24. Информационная безопасность компьютерной сети. Защита от анализаторов протоколов.

25. Значение и современные методы шифрования информации в информатизированном обществе.

26. Методологические основы технологии шифрования программными средствами.

27. Применение и проблемы стандартизации криптографических алгоритмов.

28. Средства безопасности ОС Windows 2000. Понятия и термины защиты данных. Характеристики безопасности.

29. Средства безопасности ОС Windows 2000. Применение шифрования с открытым и закрытым ключами.

30. Средства безопасности ОС Windows 2000. Алгоритмы и компоненты Windows 2000 обеспечивающие шифрование данных.

31. Средства безопасности ОС Windows 2000. Протокол аутентификации Kerberos. Основы применения протокола Kerberos.

32. Средства безопасности ОС Windows 2000. Характеристика протоколов обмена сообщениями.

33. Аутентификация протокола Kerberos в доменах ОС Windows 2000.

34. Шифрующая файловая система EPS и ее архитектура.

35. Средства безопасности ОС Windows 2000. Применение EPS в ОС Windows 2000.

36. Средства безопасности ОС Windows 2000. Шифрование файлов и каталогов. Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок.

37. Средства безопасности ОС Windows 2000. Архивация и восстановление зашифрованных файлов на другом компьютере.

38. Средства безопасности ОС Windows 2000. Восстановление данных, зашифрованных с помощью неизвестного личного ключа.

39. Протокол безопасности IP в ОС Windows 2000. Характеристика средств безопасности протокола IP.

40. Архитектура протокола безопасности IP в ОС Windows 2000.

41. Разработка плана безопасности IP в ОС Windows 2000.

42. Администрирование безопасности в ОС Windows 2000.

43. Использование сертификатов для обеспечения безопасности в ОС Windows 2000. Хранилища сертификатов безопасности.

44. Планирование мероприятий по защите информации.

45. Характеристика программных средств шифрования информации.

46. Применение средства криптографической защиты информации PrettygoodPrivacy (PGP).

Шкала оценивания

Баллы (рейтинговой оценки)	**Оценка**	**Требования к знаниям**
100-40	*Зачтено*	- Оценка «зачтено» выставляется студенту, если он продемонстрировал: на уровне знаний: классификация угроз по информационным ресурсам; современные проблемы информационной безопасности; основные концептуальные положениями системы защиты информации; основные направления обеспечения информационной безопасности; на уровне умений: меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи; на уровне навыков: использование современных методов защиты информации в компьютерных системах; осуществление мероприятий по обеспечению
39-0	*Не зачтено*	Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. – Учебные достижения в семестровый период и результатами рубежного контроля демонстрировали не высокую степень овладения программным материалом по минимальной планке.

4.4.Методические материалы

Занятия по дисциплине «Информационная безопасность» представлены следующими видами работы: лекции, практические, а также самостоятельной работой студентов.

На практических занятиях студенты выполняют задания, связанные с расчетом основных показателей, с обсуждением проблемных вопросов и вырабатывают свое мнение по поводу решения основных экономических вопросов в сфере информационной безопасности.

В рамках самостоятельной работы студенты готовятся по вопросам, готовятся к семинарским занятиям, осуществляют подготовку к зачету.

Текущая аттестация по дисциплине «Информационная безопасность»проводится в форме тестирования и подготовки рефератов по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

– учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

– степень усвоения теоретических знаний;

– уровень овладения практическими умениями и навыками по всем видам учебной работы;

– результаты самостоятельной работы.

Активность студента на занятиях оценивается по его выступлениям по вопросам практических занятий, ответах при представлении рефератов, тестировании и др.

Промежуточная аттестация студентов по дисциплине «Информационная безопасность» проводится в соответствии с Уставом Академии, Положением о промежуточной аттестации студентов по программам ВО. Промежуточная аттестация по дисциплине проводится в соответствии с Учебным планом в форме зачета.

Оценка ***работы студента на семинарских занятиях*** осуществляется по следующим критериям:

– отлично - активное участие в обсуждении проблем каждого семинара, самостоятельность ответов, свободное владение материалом, полные и аргументированные ответы на вопросы семинара, участие в дискуссиях, твёрдое знание лекционного материала, обязательной и рекомендованной дополнительной литературы, регулярная посещаемость занятий.

– хорошо - недостаточно полное раскрытие некоторых вопросов темы, незначительные ошибки в формулировке категорий и понятий, меньшая активность на семинарах, неполное знание дополнительной литературы, хорошая посещаемостью.

– удовлетворительно - ответы отражают в целом понимание темы, знание содержания основных категорий и понятий, знакомство с лекционным материалом и рекомендованной основной литературой, недостаточная активность на занятиях, оставляющая желать лучшего посещаемость.

– неудовлетворительно - пассивность на семинарах, частая неготовность при ответах на вопросы, плохая посещаемость, отсутствие качеств, указанных выше для получения более высоких оценок.

Критерии оценивания тестов

Критерии выставления оценок за тест, состоящий из пяти вопросов.
Время выполнения работы: 7-10 мин.
Оценка **«отлично»** –5 правильных ответов;
Оценка **«хорошо»** –4 правильных ответов;
Оценка **«удовлетворительно»** –3 правильных ответов;
Оценка **«неудовлетворительно»** –2 правильных ответов.

Критерии выставления оценок за тест, состоящий из десяти вопросов.
Время выполнения работы: 10-15 мин.

Оценка **«отлично»** –10 правильных ответов;
Оценка **«хорошо»** –9-7 правильных ответов;
Оценка **«удовлетворительно»** –6-5 правильных ответов;
Оценка **«неудовлетворительно»** –менее 5 правильных ответов.

Критерии выставления оценок за тест, состоящий из пятнадцати заданий.
Время выполнения работы: 15-20 мин.
Оценка **«отлично»** –15-14 правильных ответов;
Оценка **«хорошо»** –13-10 правильных ответов;
Оценка **«удовлетворительно»** –9-7 правильных ответов;
Оценка **«неудовлетворительно»** –менее 6 правильных ответов.

Критерии оценивания реферата

Оценка **«отлично»** выставляется студенту, если содержание реферата соответствует заявленной в названии тематике; реферат оформлен в соответствии с общими требованиями написания и техническими требованиями оформления реферата; реферат имеет чёткую композицию и структуру; в тексте реферата отсутствуют логические нарушения в представлении материала; корректно оформлены и в полном объёме представлены список использованной литературы и ссылки на использованную литературу в тексте реферата; отсутствуют орфографические, пунктуационные, грамматические, лексические, стилистические и иные ошибки в авторском тексте; реферат представляет собой самостоятельное исследование, представлен качественный анализ найденного материала, отсутствуют факты плагиата.

Оценка **«хорошо»** выставляется студенту**,** если содержание реферата соответствует заявленной в названии тематике; реферат оформлен в соответствии с общими требованиями написания реферата, но есть погрешности в техническом оформлении; реферат имеет чёткую композицию и структуру; в тексте реферата отсутствуют логические нарушения в представлении материала; в полном объёме представлены список использованной литературы, но есть ошибки в оформлении; корректно оформлены и в полном объёме представлены ссылки на использованную литературу в тексте реферата; отсутствуют орфографические, пунктуационные, грамматические, лексические, стилистические и иные ошибки в авторском тексте; реферат представляет собой самостоятельное исследование, представлен качественный анализ найденного материала, отсутствуют факты плагиата.

Оценка **«удовлетворительно»,** если содержание реферата соответствует заявленной в названии тематике; в целом реферат оформлен в соответствии с общими требованиями написания реферата, но есть погрешности в техническом оформлении; в целом реферат имеет чёткую композицию и структуру, но в тексте реферата есть логические нарушения в представлении материала; в полном объёме представлен список использованной литературы, но есть ошибки в оформлении; некорректно оформлены или не в полном объёме представлены ссылки на использованную литературу в тексте реферата; есть единичные орфографические, пунктуационные, грамматические, лексические, стилистические и иные ошибки в авторском тексте; в целом реферат представляет собой самостоятельное исследование, представлен анализ найденного материала, отсутствуют факты плагиата.

Оценка **«неудовлетворительно»,** если содержание реферата соответствует заявленной в названии тематике; в реферате отмечены нарушения общих требований, написания реферата; есть погрешности в техническом оформлении; в целом реферат имеет чёткую композицию и структуру, но в тексте реферата есть логические нарушения в представлении материала; в полном объёме представлен список использованной литературы, но есть ошибки в оформлении; некорректно оформлены или не в полном объёме представлены ссылки на использованную литературу в тексте реферата; есть частые орфографические, пунктуационные, грамматические, лексические, стилистические и иные ошибки в авторском тексте; в целом реферат представляет собой достаточно самостоятельное исследование, представлен анализ найденного материала, присутствуют единичные случаи фактов плагиата.

5. Методические указания для обучающихся по освоению дисциплины

Практические занятия дисциплины предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения студент должен готовиться к лекции, т.к. она является важнейшей формой организации учебного процесса, поскольку:

– знакомит с новым учебным материалом;
– разъясняет учебные элементы, трудные для понимания;
– систематизирует учебный материал;
– ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем:

– внимательно прочитайте материал предыдущей лекции;
– узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);
– ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
– постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
– запишите возможные вопросы, которые вы зададите лектору на лекции.

Подготовка к практическим занятиям:

– внимательно прочитайте материал лекций относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
– выпишите основные термины;
– ответьте на контрольные вопросы по семинарским занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;
– уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до семинарского занятия) во время текущих консультаций преподавателя;
– готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;
– рабочая программа дисциплины в части целей, перечню знаний, умений, терминов и учебных вопросов может быть использована вами в качестве ориентира в организации обучения.

Подготовка к зачету. К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают не слишком удовлетворительные результаты. В самом начале изучения учебной дисциплины познакомьтесь со следующей учебно-методической документацией:

– программой дисциплины;
– перечнем знаний и умений, которыми студент должен владеть;
– тематическими планами лекций, семинарских занятий;
– контрольными мероприятиями;
– учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
– перечнем вопросов к зачету.

После этого у вас должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета.

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости, время подготовки может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на лекциях звукозаписывающих устройств. Допускается присутствие на занятиях ассистента, оказывающего обучающимся необходимую техническую помощь. Оценка знаний студентов на семинарских занятиях осуществляется в устной форме (как ответы на вопросы, так и практические задания).

Промежуточная аттестация для лиц с нарушением зрения проводится устно, при этом текст заданий предоставляется в форме адаптированной для лиц с нарушением зрения (укрупненный шрифт), при оценке используются общие критерии оценивания. При необходимости, время подготовки может быть увеличено.

Лица с нарушениями опорно-двигательного аппарата не нуждаются в особых формах предоставления учебных материалов. Однако, с учетом состояния здоровья часть занятий может быть реализована дистанционно (при помощи сети «Интернет»). Так, при невозможности посещения лекционного занятия студент может воспользоваться кратким конспектом лекции. При невозможности посещения практического занятия студент должен предоставить письменный конспект ответов на вопросы, письменно выполненное практическое задание. Доклад так же может быть предоставлен в письменной форме (в виде реферата), при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями опорно-двигательного аппарата проводится на общих основаниях, при необходимости процедура может быть реализована дистанционно (например, при помощи программы Skype). Для этого по договоренности с преподавателем студент в определенное время выходит на связь для проведения

процедуры. В таком случае вопросы и практическое задание выбираются самим преподавателем.

Содержание самостоятельной работы студентов

Самостоятельная работа студентов предполагает выполнение ими таких учебных заданий как подготовка и выступление с докладом и написание реферата по избранной теме. Уровень выполненной работы учитывается преподавателем при приеме зачета. Отдельные, наиболее интересные рефераты могут быть заслушаны.

При выступлении с докладом студент должен: свободно владеть излагаемым материалом; уметь отвечать на поставленные вопросы.

Реферат должен отвечать следующим требованиям: иметь четкий краткий план, внятное изложение материала, собственное видение проблемы, грамотное оформление списка литературы. Объем может составлять 15-20 рукописных страниц.

Общий перечень самостоятельной работы

Рекомендуется следующие виды самостоятельной работы:

- конспектирование учебных материалов;
- составление тезисов;
- составление логических схем;
- подготовка докладов и рефератов по заданной тематике.

Перечень тем, изучаемых студентами самостоятельно

1. Актуальность информационной безопасности.
2. Лицензирование и сертификация в области защиты информации.
3. Основные нормативные руководящие документы.
4. Информационная безопасность сетей.
5. Способы совершения компьютерных преступлений.
6. Уязвимость сети Интернет.
7. Компьютерные преступления.
8. Вредоносные программы.
9. Вирусы.
10. Теория информационной безопасности информационных систем.
11. Криптографические способы защиты информации.
12. Организация информационной безопасности компании.
13. Обеспечения информационной безопасности.
14. Контроль доступа к информации.
15. Методы и средства защиты информации.
16. Антивирусное ПО.

6. Основная и дополнительная учебная литература, необходимая для освоения дисциплины (модуля), ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1.Артемов А.В. Информационная безопасность. МАБИВ, 2014. http://www.iprbookshop.ru/33430

2. Милославская Н.Г. Управление рисками информационной безопасности. Горячая линия, 2012. http://www.iprbookshop.ru/12060

3. Шаньгин В.Ф. Информационная безопасность и защита информации. ДМК Пресс, 2014. http://www.iprbookshop.ru/29257

6.2. Дополнительная литература

1.Белов Е.Б. Основы информационной безопасности. Горячая линия-Телеком, 2011. http://www.iprbookshop.ru/12014.html

2. Данжани Н, Кларк Д.Средства сетевой безопасности/ Пер с англ.- СПб.: КУДИЦ-ПРЕСС, 2007.-368с.

3. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М: Логос; ПБОЮЛ Н.А. Егоров, 2001. - 264с.

6.3. Учебно-методическое обеспечение самостоятельной работы

1. Максим М., Поллино Д. Безопасность беспроводных сетей - М.: ДМК Пресс, 2008. - 283 с. - http://www.biblioclub.ru

2. ТорстейнсонП.Криптография и безопасность в технологии .NET/П. Торстейнсон, Г.А. Ганеш; пер. с англ. - М: БИНОМ. Лаборатория знаний, 2007. - 479с.

6.4. Нормативные правовые документы

Не используются.

6.5. Интернет-ресурсы.

1. www.nnir.ru / - Российская национальная библиотека
2. www.nns.ru / -Национальная электронная библиотека
3. www.rsi.ru / - Российская государственная библиотека
4. www.yandex.ru / - Поисковая система
5. http://www.consultant.ru/ - Консультант плюс
6. http://www.garant.ru/ - Гарант
7. БДИ: Безопасность, Достоверность, Информация.
8. Безопасность информации.
9. Бизнес и безопасность в России.
10. Вопросы защиты информации (Всероссийский научно-исследовательский институт межотраслевой информации).
11. Делопроизводство (ЗАО «Бизнес-Школа «Интел-Синтез»).
12. Документоведение, документационное обеспечение управления (библиографический указатель и экспресс-информация ОЦНТИДАД ВНИИДАД ГАС РФ)

13. Защита информации. Конфидент.
14. Мир безопасности.
15. Системы безопасности (Компания «Гротек»).
16. Секретарское дело (ЗАО «Бизнес-Школа «Интел-Синтез»).
17. Секьюрити.
18. Телохранитель.
19. Частный сыск, охрана, безопасность (Интерпол Москва, Издательский дом «Мир безопасности»).
20. Records Management Quarterly
21. Security Management
22. Security Industry and Product New

6.6. Иные источники

Не используются.

7. Материально-техническая база, информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Специальные помещения представляют собой 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. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочим учебным программам дисциплин.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.

Академия проводит постоянную работу по созданию и системному улучшению условий получения образования людьми с ограниченными возможностями здоровья. В настоящее время здания и территории Академии оснащены лифтами для перевозки инвалидов в колясках, порядка 80% аудиторий и компьютерных классов имеют двери, соответствующие требованиям нормативов, оборудованы пандусы при входе в здания, а также внутри учебных корпусов и общежития, имеются специальные туалеты.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде организации. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-

телекоммуникационной сети «Интернет», как на территории организации, так и вне ее.

Академия обеспечена необходимым комплектом лицензионного программного обеспечения.

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам.

Обучение лиц с ограниченными возможностями здоровья осуществляется с учетом индивидуальных психофизических особенностей, а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида. Для лиц с нарушением слуха возможно предоставление информации визуально (краткий конспект лекций, основная и дополнительная литература), на лекционных и практических занятиях допускается присутствие ассистента.

Оценка знаний студентов на практических занятиях осуществляется на основе письменных конспектов ответов на вопросы, письменно выполненных практических заданий. Доклад так же может быть предоставлен в письменной форме (в виде реферата), при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Организован доступ к следующим электронным ресурсам:

Bloomberg

EBSCO Publishing

eLIBRARY.RU

Emerging Markets Information Service

Google Scholar (Google Академия)

IMF eLibrary -

JSTOR

New Palgrave Dictionary of Economics – Электронный словарь.

OECD iLibrary

Oxford Handbooks Online

Polpred.com Обзор СМИ

Science Direct - Журналы издательства Elsevier по экономике и эконометрике, бизнесу и финансам, социальным наукам и психологии, математике и информатике;

SCOPUS

Web of Science

Wiley Online Library

World Bank Elibrary

Архивы научных журналов NEICON

Интернет-сервис «Антиплагиат»

Система Профессионального Анализа Рынков и Компаний «СПАРК»

ЭБС Издательства "Лань"
ЭБС Юрайт
Электронная библиотека Издательского дома «Гребенников»