Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
Факультет журналистики

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Иванов А.Г.
подпись
«__» _____ 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ФТД.В. 01 Основы информационной безопасности
(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки/специальность 42.03.03 Издательское дело
(код и наименование направления подготовки/специальности)

Направленность (профиль) / специализация
Редакционно-издательская деятельность
(наименование направленности (профиля) специализации)

Программа подготовки академическая
(академическая /прикладная)

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

Квалификация (степень) выпускника бакалавр
(бакалавр, магистр, специалист)

Краснодар 2015

Рабочая программа дисциплины ФТД. В. 01 Основы информационной безопасности составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 42.03.03 Издательское дело
код и наименование направления подготовки

Программу составил(и):
Хлопунова О.В. доцент, канд. филолог наук доцент _____
И.О. Фамилия, должность, ученая степень, ученое звание подпись

Рабочая программа дисциплины ФТД. В. 01 Основы информационной безопасности утверждена на заседании кафедры издательского дела, рекламы и медиатехнологий
протокол № 8 «22» апреля 2015 г.
Заведующий кафедрой (разработчика) Кравченко Н.П. _____
фамилия, инициалы подпись

Рабочая программа обсуждена на заседании кафедры издательского дела, рекламы и медиатехнологий
протокол № 8 «22 » апреля 2015 г.
Заведующий кафедрой
издательского дела и медиатехнологий Кравченко Н.П. _____
фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии факультета
протокол № 09-15 «26» мая 2015 г.
Председатель УМК факультета Демина Л.И. _____
фамилия, инициалы подпись

Рецензенты:
(представители работодателей и академических сообществ, не менее 2-х представителей)

Г.Н. Немец канд филолог. наук доцент кафедры рекламы и связей с общественностью ФГБОУ ВО «КубГУ»

О.В. Буз генеральный директор ОАО «Печатный двор Кубани»

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Целью изучения дисциплины является изучение основных общеметодологических принципов теории информационной безопасности, формирование представления и практических навыков работы с информацией, навыков анализа угроз информационной безопасности.

1.2 Задачи дисциплины предполагают:

– ознакомление студентов с терминологией информационной безопасности;

– развитие мышления студентов;

– изучение методов и средств информационной безопасности;

– обучение определению причин и видов, источников и каналов утечки, искажения информации.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Основы информационной безопасности» относится к факультативным дисциплинам вариативной части учебного плана.

Дисциплина «Основы информационной безопасности» в соответствии с учебным планом по направлению подготовки 42.03.03 Издательское дело является промежуточным этапом в формировании и развитии компетенций, осваиваемых при изучении дисциплин «Информационные технологии в издательском деле», «Электронные средства информации», «Технологии производства печатных и электронных средств информации».

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся профессиональных компетенций (ПК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**Уметь**	**Владеть**
1.	ОПК-1	Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	терминологические основы информационной безопасности; общеметодологические принципы теории информационной безопасности	применять полученные знания, умения и навыки на практике	необходимым набором знаний по основным правовым документам, обеспечивающим процедуру соблюдения информационной безопасности
2.	ПК-16	Способностью владеть приемами и методами аналитико-синтетической переработки потоков	основные приемы и методы работы с информацией; виды угроз и	анализировать характер угроз и определять источники угроз; классифициро	методами анализа информации на предмет целостности; методами

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**Уметь**	**Владеть**
		информации	последовательность решения задачи защиты информации.	вать автоматизированных систем обработки информации по классу защиты информации	определения коэффициентов важности, полноты, адекватности, релевантности, толерантности информации.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часа), их распределение по видам работ представлено в таблице

(для студентов ОФО)

Вид учебной работы		Всего часов	Семестры (часы)			
			1			
Контактная работа, в том числе		32.2	32.2			
Аудиторные занятия (всего):		28	28			
Занятия лекционного типа		14	14			
Занятия семинарского типа (семинары, практические занятия)		14	14			
Лабораторные занятия						
Иная контактная работа:						
Контроль самостоятельной работы (КСР)						
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		39.8	39.8			
Курсовая работа		-	-			
Проработка учебного (теоретического) материала		15	15			
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		15	15			
Реферат		-	-			
Подготовка к текущему контролю		9.8	9.8			
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час**	**72**	**72**			
	в том числе контактная работа	32.2	32.2			
	зач.ед.	2	2			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 1 семестре *(очная форма)*

№	Наименование разделов (тем)	Количество часов

		Всего	Аудиторная Работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Понятие национальной безопасности, виды безопасности.		2	2	-	2
2.	Терминологические основы информационной безопасности. Основные понятия и определения		2	2	-	3
3.	Общеметодологические принципы теории информационной безопасности		2	-	-	5
4.	Угрозы. Классификация и анализ угроз информационной безопасности.		2	4	-	5
5.	Методы нарушения конфиденциальности, целостности и доступности информации		2	2	-	5
6.	Причины, виды, каналы утечки и искажения информации.		2	4	-	5
7.	Функции и задачи защиты информации		2	-	-	5
8.	Итоговое занятие. Прием зачета		-	2	-	9.8
	Итого по дисциплине:		14	14	-	39.8

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
1.	Понятие национальной безопасности, виды безопасности.	Информационная безопасность РФ. Органы обеспечивающие национальную безопасность, цели, задачи. Приоритетные направления в области защиты информации в РФ. Государственная тайна. Правовое обеспечение защиты информации.	Конспект лекции
2.	Терминологические основы информационной безопасности. Основные понятия и определения	Понятие информации, информатизации, информационных систем и смежных с ними: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации.	Конспект лекции
3.	Общеметодологические принципы теории информационной безопасности	Этапы развития информационной безопасности: 1. Системы безопасности ресурса; 2. Этап развитой защиты; 3. Этап комплексной защиты. Требования к системе защиты информации.	Конспект лекции
4.	Угрозы. Классификация и	Понятие угрозы. Виды угроз. Характер происхождения угроз (умышленные факторы,	Конспект

	анализ угроз информационной безопасности.	естественные факторы). Источники угроз. Предпосылки появления угроз: объективные, субъективные.	лекции
5.	Методы нарушения конфиденциальности, целостности и доступности информации	Классы каналов несанкционированного получения информации: непосредственно с объекта, с каналов отображения информации, получение по внешним каналам, подключение к каналам получения информации. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных. Функции защиты информации.. Стратегии защиты информации: оборонительная, наступательная, упреждающая. Архитектура систем защиты информации.	Конспект лекции
6.	Причины, виды, каналы утечки и искажения информации	Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический, теоретико-эмпирический. Модель защиты – модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Факторы, влияющие на требуемый уровень защиты информации	Конспект лекции
7.	Функции и задачи защиты информации	Методы формирования функций защиты. Сокрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Регулирование доступа к элементам системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека. Применение криптографии. Региональные компоненты защиты информации.	Конспект лекции

2.3.2 Занятия семинарского типа.

№	Наименование раздела (темы)	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.	Понятие национальной	ГОСТы и руководящие документы. Доктрина информационной безопасности	Устное сообщение/ доклад

	безопасности, виды безопасности.	РФ. ФЗ РФ «Об информации, информатизации и защите информации». ФЗ РФ «Об электронной цифровой подписи». ФЗ РФ «О техническом регулировании». ФЗ «О лицензировании отдельных видов деятельности», ФЗ «О коммерческой тайне»	
2.	Терминологические основы информационной безопасности. Основные понятия и определения	Анализ терминов и определений информационной безопасности.	Устное сообщение/ доклад/ практическое задание
3.	Угрозы. Классификация и анализ угроз информационной безопасности.	Угрозы информации. Проведение анализа информации на предмет целостности. Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации.	Устное сообщение/ доклад/практическое задание
4.	Методы нарушения конфиденциальности, целостности и доступности информации	Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации	Устное сообщение/ доклад/ практическое задание
5.	Причины, виды, каналы утечки и искажения информации	Классификация автоматизированных систем обработки информации по классу защиты информации. Оценка безопасности информации на объектах ее обработки	Устное сообщение/ доклад/практическое задание

2.3.3 Лабораторные занятия

Не предусмотрены

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1.	Проработка учебного (теоретического) материала	1. Методические рекомендации по самостоятельной работе студентов. В.Ю. Кожанова, Кубанский государственный университет. Краснодар, 2012 г 2. Прохорова, О.В.Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - http://biblioclub.ru/index.php?page=book&id=438331. 3. Галатенко,В.АСтандарты **информационной безопасности** [Текст] : курс лекций : учебное пособие для студентов вузов / В. А. Галатенко

		; под ред. В. Б. Бетелина. - 2-е изд. - М. : Интернет-Университет Информационных Технологий, 2006. - 263 с (40 экз) 4. Галатенко, В. А.**Основы информационной безопасности** [Текст] : курс лекций : для студентов вузов / В. А. Галатенко ; под ред. В. Б. Бетелина. - М. : Интернет-Университет Информационных Технологий, 2003. (50 экз).
2.	Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	1. Методические рекомендации по самостоятельной работе студентов. В.Ю. Кожанова, Кубанский государственный университет. Краснодар, 2012 г 2. Основы информационной безопасности [Электронный ресурс] : курс лекций : учебное пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. - Мзд. 3-е. - М. : Интернет-Университет Информационных Технологий, 2006. - 2-8 с. - https://biblioclub.ru/index.php?page=book_red&id=233063&sr=1. 3. Галатенко,В.А.Стандарты **информационной безопасности** [Текст] : курс лекций : учебное пособие для студентов вузов / В. А. Галатенко ; под ред. В. Б. Бетелина. - 2-е изд. - М. : Интернет-Университет Информационных Технологий, 2006.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии.

В ходе освоения дисциплины «Основы информационной безопасности» используются актуальные образовательные технологии с использованием современного технического оснащения и программного обеспечения учебного процесса.

Применяются активные и интерактивные формы проведения занятий: лекция-беседа, семинары с использованием презентации.

Формой контроля знаний является зачет, который содержит следующие формы работы:

- самостоятельная работа (презентация, доклад) для контроля освоения теоретического курса дисциплины;
- практические задания для выявления степени овладения базовыми практическими навыками;
- ответы на вопросы по темам основных разделов дисциплины.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

4.1.1. Примерная тематика устных сообщений/ докладов:

1. Безопасность в информационном обществе.
2. Информация в современном обществе и ее свойства.
3. Информационная война как угроза национальной безопасности.
4. Место информационной безопасности в системе национальной безопасности.
5. Значение информационной безопасности для субъектов информационных отношений.
6. Концептуальная модель информационной безопасности РФ и основные понятия.
7. Политика обеспечения информационной безопасности РФ.

Национальные интересы России в информационной сфере и их безопасность.

8. Объекты. Подлежащие защите от потенциальных угроз и противоправных посягательств.
9. Виды и источники угроз информационной безопасности РФ.
10. Компьютерные преступления. Классификация. Способы совершенствования компьютерных преступлений.
11. Причины уязвимости Интернет. Злоумышленники в Интернет.
12. Вредоносные программы. Условия существования вредоносных программ.
13. Классические компьютерные вирусы. Способы внедрения вирусов.
14. Защита от компьютерных вирусов. Признаки заражения компьютера. Источники компьютерных вирусов.
15. Защита от компьютерных вирусов. Основные правила защиты. Антивирусные программы.
16. Методы и средства защиты компьютерной информации. Классификация мер обеспечения безопасности компьютерных систем.
17. Методы обеспечения информационной безопасности РФ.
18. Методы и средства защиты информации от случайных воздействий, от аварийных ситуаций, от утечки за счет побочного электромагнитного излучения и наводок
19. Организационные мероприятия по защите информации.
20. Организация информационной безопасности компании.
21. Информационное страхование.
22. Криптографические методы информационной безопасности.
23. Лицензирование в области защиты информации.
24. Сертификация в области защиты информации.
25. Аттестация в области защиты информации.
26. Критерии безопасности компьютерных систем «Оранжевая книга».
27. Руководящие документы Гостехкомиссии.
28. Объекты и угрозы информационной безопасности организации.
29. Система обеспечения информационной безопасности организзции.
30. Модель информационной безопасности организации.

4.1.2 Примеры практических задач:

Задание 1

Выбрать объект защиты информации (одиночный стоящий в бухгалтерии компьютер; сервер в бухгалтерии; почтовый сервер; веб-сервер и т.д.). Описать объект защиты, провести анализ защищенности объекта по следующим пунктам:

1. Виды угроз.
2. Характер происхождения угроз.
3. Классы каналов несанкционированного получения информации.

4. Источники появления угроз.
5. Причины нарушения целостности информации.
6. Потенциально возможные злоумышленные действия.
7. Определить класс защиты информации.

Задание 2

Предложить анализ увеличения защищенности объекта защиты информации по следующим пунктам:

1. Определить требования к защите информации.
2. Классифицировать автоматизированную систему.
3. Определить факторы, влияющие на требуемый уровень защиты информации.
4. Выбрать или разработать способы и средства защиты информации.
5. Построить архитектуру системы защиты информации.
6. Сформулировать рекомендации по увеличению уровня защищенности.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

ФОС для проведения промежуточной аттестации обучающихся по дисциплине предназначен для оценки степени достижения запланированных результатов обучения по завершению изучения дисциплины в установленной учебным планом форме и позволяет определить качество усвоения изученного материала. Подготовка студента к прохождению промежуточной аттестации осуществляется в период лекционных и семинарских занятий, а также во внеаудиторные часы в рамках самостоятельной работы. Во время самостоятельной подготовки студент пользуется конспектами лекций, основной и дополнительной литературой по дисциплине.

Итоговой формой контроля сформированности компетенций у студентов по дисциплине является – зачет.

4.2.1 Вопросы для зачета по дисциплине «Основы информационной безопасности»:

1. Теория защиты информации. Основные определения.
2. Обеспечение информационной безопасности и направление защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная).
4. Требования к системе защиты информации.
5. Угрозы информации.
6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки появления угроз.
9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.
14. Общая модель процесса нарушения физической целостности информации.
15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
16. Методологические подходы к оценке уязвимости информации.
17. Модель защиты системы с полным перекрытием.
18. Рекомендации по использованию моделей оценки уязвимости информации.

19. Допущения в моделях оценки уязвимости информации.
20. Методы определения требований к защите информации.
21. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
22. Классификация требований к средствам защиты информации.
23. Требования к защите, определяемые структурной автоматизированной системы обработки данных
24. Требования к защите, обусловливаемые видом защищаемой информации.
25. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.
26. Анализ существующих методик определения требований к защите информации.
27. Факторы, влияющие на требуемый уровень защиты информации.
28. Способы и средства защиты информации.
29. Способы «абсолютной защиты».
30. Архитектура системы защиты информации. Требования.
31. Построение средств защиты информации.
32. Ядро системы защиты информации.

4.2.2 Критерии оценивания

Оценка «зачтено». Выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал различной литературы, правильно обосновывает принятое нестандартное решение, владеет разносторонними навыками и приемами выполнения практических задач по формированию общепрофессиональных компетенций.

Оценка «не зачтено». Выставляется студенту, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения практической работы.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

1.1 Основная литература:

5. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов – URL: https://e.lanbook.com/book/5121#book_name
6. Нестеров С.А. Основы информационной безопасности. учебное пособие. – URL: https://e.lanbook.com/book/103908#book_name

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература:

1 Прохорова, О.В.Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - http://biblioclub.ru/index.php?page=book&id=438331.

2 Галатенко,В.АСтандарты **информационной безопасности** [Текст] : курс лекций : учебное пособие для студентов вузов / В. А. Галатенко ; под ред. В. Б. Бетелина. - 2-е изд. - М. : Интернет-Университет Информационных Технологий, 2006. - 263 с (40 экз)

5.3.Периодические издания.

Не требуется.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

1 Основы информационной безопасности [Электронный ресурс] : курс лекций : учебное пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. - Мзд. 3-е. - М. : Интернет-Университет Информационных Технологий, 2006. - 2-8 с. - https://biblioclub.ru/index.php?page=book_red&id=233063&sr=1.

2 Галатенко, В. А.**Основы информационной безопасности** [Текст] : курс лекций : для студентов вузов / В. А. Галатенко ; под ред. В. Б. Бетелина. - М. : Интернет-Университет Информационных Технологий, 2003. (50 экз).

7. Методические указания для обучающихся по освоению дисциплины (модуля).

Важнейшей составной частью освоения курса является посещение лекций (обязательное) и их конспектирование.

Лекционные занятия (Л).

Лекции являются аудиторными занятиями, которые рассчитаны на максимальное использование творческого потенциала слушателей.

Вузовская лекция – главное звено дидактического цикла обучения. Её цель – формирование у обучающихся ориентировочной основы для последующего усвоения материала методом самостоятельной работы. Содержание лекции должно отвечать следующим дидактическим требованиям:

– изложение материала от простого к сложному, от известного к неизвестному;

– логичность, четкость и ясность в изложении материала;

– возможность проблемного изложения, дискуссии, диалога с целью активизации деятельности обучающихся в ходе лекции;
– опора смысловой части лекции на подлинные факты, события, явления, статистические данные;
– тесная связь теоретических положений и выводов с практикой и будущей профессиональной деятельностью обучающихся;
– научность и информативность (современный научный уровень), доказательность и аргументированность, наличие достаточного количества ярких, убедительных примеров, фактов, обоснований, документов и научных доказательств;
– активизация мышления слушателей, постановка вопросов для размышления, четкая структура и логика раскрытия последовательно излагаемых вопросов;
– разъяснение вновь вводимых терминов и названий, формулирование главных мыслей и положений, подчеркивание выводов, повторение их;
– эмоциональность формы изложения, доступный и ясный язык.

Глубокому освоению лекционного материала способствует предварительная подготовка, включающая чтение предыдущей лекции, работу со словарями, энциклопедиями, учебниками, ГОСТами.

Самостоятельная работа является составной частью процесса качественного и полного усвоения учебной программы по курсу и тесно связана с аудиторными занятиями. В ходе самостоятельной работы студенты изучают менее трудные темы и вопросы, которые с достаточной степенью глубины и полноты освещены в соответствующих учебниках, учебных пособиях, монографиях, научных статьях и иных источниках. При проработке конкретной темы студенту необходимо внимательно прочесть рекомендуемую литературу, уяснить концепцию, систему аргументации и структуру материала, после чего сделать конспект полученной информации в виде кратких тезисов. Следует также сопоставить полученные в результате самостоятельной работы знания с содержанием аудиторных занятий.

Оценивание результатов обучения студентов по дисциплине «Основы информационной безопасности» осуществляется по регламентам текущего контроля и промежуточной аттестации.

Текущий контроль в семестре проводится с целью обеспечения своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы студентов. Объектом текущего контроля являются конкретизированные результаты обучения (учебные достижения) по дисциплине. Текущий контроль предусматривает проведение следующих мероприятий:

– подготовка устных сообщений/докладов;

– выполнение практических заданий по предложенным преподавателем темам.

Индивидуальное сообщение (доклад) – вид самостоятельной работы, предполагающий устное выступление. При подготовке индивидуального сообщения по заданной теме на первом этапе необходимо составить план, подобрать основные источники, затем в процессе работы с научной литературой систематизировать полученную информацию, сделать выводы и обобщения. Устное выступление должно хорошо восприниматься на слух, поэтому необходимо контролировать темп речи. Текст сообщения должен быть построен в соответствии с регламентом предстоящего выступления. Выводы должны быть максимально четкими и краткими, для этого рекомендуется их пронумеровать или изложить тезисно. После выступления докладчик должен ответить на вопросы слушателей. Индивидуальное сообщение не может быть оценено положительно, если в нем поверхностно раскрыты вопросы, допущены принципиальные ошибки, докладчик не смог уложиться в регламент или ответить на вопросы, речевое оформление сообщения не соответствует нормам и правилам русского литературного языка, а также при условии механического копирования материала из

учебников или другой литературы. В качестве иллюстративной поддержки рекомендуется сопровождение доклада презентацией.

Презентация – это сжатое изложение информации по проблеме, актуальной для профессиональной деятельности. Подготовка презентации предполагает сбор информации по проблеме из различных источников, анализ полученных данных и их обобщенное изложение в виде слайдов. Доклад по подготовленной презентации исключает дословное чтение слайдов. Презентация составляется в программе Microsoft Power Point. Количество слайдов определяется структурой ответа на вопрос, сформулированный в теме. Слайды оформляются в единой цветовой гамме, оформление определяется одним из форматов, предлагаемых конструктором программы. Фотографии и рисунки непременно подписываются. Если студент не является автором текста, а приводит его дословно или в пересказе, пользуется статистическими данными, то необходимо привести библиографическое описание источника с указанием автора/авторов, дать ссылку на страницы цитируемого издания, указать электронный адрес материала в сети Интернет. Список источников и материалов из сети Интернет оформляется в соответствии с нормами составления библиографического описания (см. методические указания к оформлению курсовых и дипломных работ)

Практические задания направлены на подтверждение теоретических положений и формирование учебных и профессиональных практических умений и составляют важную часть теоретической и профессиональной практической подготовки.

Выполнению заданий предшествует самостоятельное изучение студентом специальной литературы по теме. Затем на занятиях в аудитории студенты под руководством преподавателя приступают к выполнению практических заданий, которые имеют поисковый характер и направлены на решение новой для студентов для них проблемы с опорой на имеющиеся у них теоретические знания.

Промежуточный контроль (зачет) предназначен для объективного подтверждения и оценивания достигнутых результатов обучения после завершения изучения дисциплины.

Зачет является заключительным этапом процесса формирования компетенций студента при изучении дисциплины или ее части и имеет целью проверку и оценку знаний студентов по теории и применению полученных знаний, умений и навыков.

Для получения положительной оценки на зачете студент должен продемонстрировать знание основных понятий и терминов науки о чтении, понимать сущность и значение социально-психологического воздействия книги на читателя; современных концепций читательского восприятия; социологических и психологических характеристик читательской аудитории и средств массовой коммуникации, их роль в определении стратегии издательской деятельности. А также должен уметь применять полученные теоретические знания на практике.

При оценке ответа студента на вопрос преподаватель руководствуется следующими критериями:

- полнота и правильность ответа;
- степень осознанности, понимания изученного;
- языковое и речевое оформление ответа.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

8.1 Перечень информационных технологий.

1. Проверка домашних заданий и консультирование посредством электронной почты.
2. Использование электронных презентаций при проведении практических занятий.

8.2 Перечень необходимого программного обеспечения.

1. Microsoft Microsoft Windows 8, 10 "№73–АЭФ/223-ФЗ/2015 Соглашение Microsoft ESS 72569510"XX.11.2015 "Операционная система (Интернет, просмотр видео, запуск прикладных программ)"

2. Microsoft Microsoft Office Professional Plus "№73–АЭФ/223-ФЗ/2015Соглашение Microsoft ESS 72569510"XX.11.2015Текстовый редактор, табличный редактор, редактор презентаций, СУБД, дополнительные офисные инструменты, клиент электронной почты

8.3 Перечень необходимых информационных справочных систем

ЭБС Издательства «Лань» http://e.lanbook.com/ ООО Издательство «Лань» Договор № 370-АЭФ/2014 от 2 декабря 2014г.
ЭБС «Университетская библиотека онлайн» www.biblioclub.ru ООО «Директ-Медиа» :
Договор № 0303/2015 от 3 марта 2015г.
Договор № 2207/2015 от 22 июля 2015г
ЭБС «ZNANIUM.COM» http://www.znanium.com/ ООО «НИЦ ИНФРА-М» Договор № 0711/2014/3 от 7 ноября 2014.
ЭБС Издательства «Лань» http://e.lanbook.com/ ООО Издательство «Лань» Договор № 77/2015 от 11 ноября 2015 г.
ЭБС «Университетская библиотека онлайн» www.biblioclub.ru ООО «Директ-Медиа» Договор № 2611/2015 от 26 ноября 2015г.
ЭБС BOOK.ru http://www.book.ru/ ООО «КноРус медиа» Договор № 2311/2015 от 23 ноября 2015 г.
ЭБС «Юрайт» http://www.biblio-online.ru ООО Электронное издательство «Юрайт» Договор № 1401/2016 от 14 января 2016 г.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю).

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитории: 202, 205, 302, 402 (мультимедийны проектор, комплект учебной мебели, доска учебная), 209, 309, 411(комплект учебной мебели, доска учебная).
2.	Семинарские занятия	Аудитории: 304, 305, 306, 408 (комплект учебной мебели, доска учебная).
3.	Групповые (индивидуальные) консультации	Аудитории: 208 (имеется выход в интернет, комплект учебной мебели), 411 (комплект учебной мебели, доска учебная), 412 **(**Мультимедийная аудитория с выходом в ИНТЕРНЕТ: комплект учебной мебели доска учебная.; ПЭВМ учебная - 3 шт.; ПЭВМ преподавателя 1 шт., комплект аудиозаписывающего оборудования, микшерный пульт, коплект видеозаписывающего оборудования**)**
4.	Текущий контроль, промежуточная аттестация	Аудитории: 304, 305, 306, 408 (комплект учебной мебели, доска учебная)
5.	Самостоятельная работа	Аудитории: 301 **(**мультимедийная аудитория с выходом в ИНТЕРНЕТ: комплект учебной мебели - 16 шт.; доска учебная.; ПЭВМ учебная - 14 шт.; ПЭВМ преподавателя 1 шт., проектор); 307 (комплект учебной мебели, доска учебная)