Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Новгородский государственный университет имени Ярослава Мудрого»
Гуманитарный институт

Кафедра истории России и архивоведения

УТВЕРЖДАЮ:
Директор ИГУМ
А.А.Кузьми
«16» октября 2014г.

Информационная безопасность и защита информации

Дисциплина по направлению
034700.62 – «Документоведение и архивоведение»

Рабочая программа

СОГЛАСОВАНО:
Начальник учебного отдела
Н.Г. Федотова
«16» октября 2014 г.

Разработал:
Доцент НовГУ
Т. М. Воронина
«26» сентября 2014 г.

Принято на заседании кафедры
Истории России и архивоведения
Протокол № 1 от 14.10 2014 г.
Заведующий кафедрой
Е.В. Торопова
«16» октября 2014 г.

Великий Новгород
2014

1. Цель и задачи дисциплины

Цель дисциплины – изучение комплекса проблем информационной безопасности организаций и учреждений различных типов и направлений деятельности, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности и сохранности информационных ресурсов.

Задачи, решение которых обеспечивает достижение цели:

- овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности;
- изучение законодательных актов и нормативно-методических документов, регламентирующих данную сферу деятельности;
- освоение методов защиты информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения.

2. Место дисциплины в структуре ООП направления подготовки

Дисциплина «Информационная безопасность и защита информации» входит в базовую часть профессионального цикла основной образовательной программы по направлению подготовки 034700.62 «Документоведение и архивоведение» и читается в 6 семестре.

В соответствии с базовым учебным планом ООП, данная дисциплина базируется на ранее изученных курсах, таких как «Основы правовых знаний в сфере документоведения и архивоведения», «Архивоведение», «Информационное право».

В процессе дальнейшего обучения студентов знания, полученные при изучении «Информационной безопасности и защиты информации», будут углубляться и станут опорными при освоении последующих дисциплин, таких как: «Информационные технологии в документоведении и архивоведении», «Архивное право», «Электронные архивы», «Кадровое делопроизводство», а также при прохождении архивоведческой и преддипломной практик.

3. Требования к результатам освоения дисциплины

В результате изучения данной дисциплины студент формирует и демонстрирует следующие общекультурные и профессиональные компетенции:

- способностью использовать нормативные правовые документы в своей деятельности (ОК-6);
- способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК – 9);
- владеть основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией (ОК – 10);
- владеть базовыми знаниями в области информационных систем (языки и программные алгоритмы, компьютерный практикум) (ПК-4);

- владеть навыками использования компьютерной техники и информационных технологий в поиске источников и литературы, использовании правовых бах данных, составлении библиографических и архивных обзоров (ПК-8);
- способностью анализировать ситуацию на рынке информационных продуктов и услуг, давать экспертную оценку современным системам электронного документооборота и ведения электронного архива (ПК-15);
- владеть навыками работы с документами, содержащими информацию ограниченного доступа (ПК-32);
- владеть методами защиты информации (ПК-40);

Данная дисциплина формирует ОК и ПК, направленные на развитие навыков и умений в сфере применения информационных технологий, обеспечения информационной безопасности и защиты информации.

В результате изучения дисциплины студент должен:

- знать: законодательную и нормативно-методическую базу, регламентирующую применение информационных технологий в ДОУ и архивном деле; виды современных информационных технологий; методы, формы и средства защиты информации.

- уметь: применять на практике информационные технологии в сфере ДОУ и архивного дела; выполнять работы по информационной безопасности и защите информации; анализировать угрозы информационной безопасности.

- владеть: методами защиты информации; навыками применения технических и программных средств в ДОУ и архивном деле; навыками работы с документами, содержащими информацию ограниченного доступа.

4. Структура и содержание дисциплины

4.1. Трудоемкость дисциплины и формы аттестации

Учебная работа (УР)	Всего	Распределение по семестрам
		6
Полная трудоемкость дисциплины в зачетных единицах (З.Е.), в т.ч.: - зачет. **Распределение трудоемкости по видам УР в академических часах** (А.Ч.): - лекции - практические занятия (семинары): в том числе аудиторная СРС - внеаудиторная СРС	2 12 24 12 36	2 12 24 12 36
Аттестация: **зачет**		

4.2. Содержание дисциплины

Модуль, раздел (тема), КП/ КР	*Семестр*	*№ недели*	*Трудоемкость по видам УР (в АЧ)*				*Баллы Рейтинга*		*Рекомендуемые источники*
			лек	*Пр.*	*Ауд. СРС*	*Вне ауд. СРС*	*Пороговый*	*Максимальный*	
РАЗДЕЛ 1. ТЕМЫ И КРАТКОЕ СОДЕРЖАНИЕ	***6***	**1-4**	**4**	**4**	**2**	**8**	**11**	**22**	
1.1 Информационная безопасность как составляющая общественной безопасности	*6*	1	2	-	-	2	2	5	
1.2 Основы информационной безопасности и защиты информации – ПЗ-1	*6*	2	-	2	-	2	3	6	
1.3 Классификация информационных ресурсов – ПЗ-2	*6*	3	-	2	1	2	3	6	
1.4 Виды и особенности угроз информационной безопасности	*6*	4	2	-	1	2	3	5	
РАЗДЕЛ 2. ПРАВОВЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	***6***	**5-6**	**-**	**4**	**1**	**4**	**6**	**12**	
1.5 Правовое регулирование открытых информационных ресурсов – ПЗ-3	*6*	5	-	2	1	2	3	6	
1.6.Правовая защита информационных ресурсов ограниченного доступа	*6*	6	-	2	-	2	3	6	

- ПЗ-4									
РАЗДЕЛ 3. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ	***6***	**7-16**	**8**	**12**	**7**	**20**	**27**	**56**	
1.7 Основные направления и этапы работ по созданию комплексной системы безопасности предприятия (фирмы)	*6*	7	2	-	-	2	2	5	
1.8 Методологические основы системы безопасности предприятия (фирмы) – ПЗ-5	*6*	8	-	2	1	2	3	6	
1.9 Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов – ПЗ-6	*6*	9	-	2	-	2	3	6	
1.10 Защита информации при проведении совещаний и переговоров по конфиденциальным вопросам, приеме посетителей.	*6*	10	2	-	1	2	2	5	
1.11 Особенности работы с персоналом, владеющим конфиденциальной информацией									
1.11.1 Особенности подбора персонала для работы с конфиденциальной информацией – ПЗ-7	*6*	11	-	2	1	2	3	6	
1.11.2 Доступ персонала к конфиденциальным сведениям, документам и базам данных. Организация работы с персоналом, обладающим конфиденциальной информацией**.**- ПЗ-8	*6*	12	-	2	1	2	3	6	
1.12. Защищенный документооборот									
1.12.1. Понятие и задачи защищённого документооборота.	*6*	13	2	-	1	2	2	5	
1.12.2. Технологические системы защиты и обработки конфиденциальных документов.- ПЗ-9	*6*	14	-	2	1	2	3	6	
1.12.3. Принципы учета конфиденциальных документов. Технология обработки подготовленных конфиденциальных документов. - ПЗ-10	*6*	15	-	2	-	2	3	6	
1.12.4 Порядок работы персонала с конфиденциальными документами. Проверка наличия документов, дел и носителей информации. Формирование и хранение	*6*	16	2	-	1	2	3	5	

конфиденциальных дел.									
РАЗДЕЛ 4. ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ И ПРОГРАММНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ	**6**	**17-18**	**-**	**4**	**2**	**4**	**6**	**10**	
1.13Инженерно-техническая защита - ПЗ-11	*6*	17	-	2	1	2	3	5	
1.14 Программные средства защиты информации в компьютерах, локальных сетях и средствах связи – ПЗ-12	*6*	18	-	2	1	2	3	5	
Итого			12	24	12	36	50	100	

4.3. Формирование компетенций студентов

№ модуля дисциплины	Трудоемкость дисциплины, АЧ	Компетенции
Раздел 1-4	48	ОК-6; ОК-9; ОК-10; ПК-4;ПК-15;ПК-32;ПК-40
Итого:	48	

5. Образовательные технологии

Образовательный процесс по дисциплине строится на основе применения следующей комбинации методов преподавания: модульно-рейтинговое, проблемное обучение и развивающее обучение. В связи с этим организация познавательной деятельности включает в себя элементы пассивного, активного и интерактивного обучения.

Реализация такого рода модели задает соответствующие формы организации образовательного процесса и выражается в использовании следующих образовательных технологий:

- лекция (вводная, информационная, проблемная, лекция-презентация);
- практическое занятие (проблемный семинар, работа в малых группах, обсуждение конкретных ситуаций, презентации индивидуальных работ);
- дискуссия (общая, тематическая);
- исследовательские (контрольная работа, анализ источника, составление сообщения, доклад);
- самостоятельная работа студентов (конспект по источнику, работа с источниками по темам дисциплины, выполнение домашних заданий);
- работа с Интернет-ресурсами.

В процессе реализации образовательных технологий предусмотрено возможное использование информационных технологий: предоставление информации, выдача рекомендаций по электронной почте, использование мультимедийных средств в лекционных и практических занятиях и т.д.

Предполагаемые формы проведения **лекционно-практических занятий** по дисциплине представлены в следующей таблице.

Тема занятий	*Форма проведения*
1.1 Информационная безопасность как составляющая общественной безопасности	Вводная информационная лекция
1.4 Виды и особенности угроз информационной безопасности	Информационно-проблемная лекция с элементами дискуссии
1.7 Основные направления и этапы работ по созданию комплексной системы безопасности предприятия (фирмы)	Информационно-проблемная лекция с элементами дискуссии
1.10 Защита информации при проведении совещаний и переговоров по конфиденциальным вопросам, приеме посетителей.	Информационно-проблемная лекция
1.12.1. Понятие и задачи защищённого документооборота.	Информационно-проблемная лекция с элементами дискуссии
1.12.4 Порядок работы персонала с конфиденциальными документами. Проверка наличия документов, дел и носителей информации. Формирование и хранение конфиденциальных дел.	Информационно-проблемная лекция, работа в малых группах

6. Оценочные средства контроля успеваемости

6.1. Формы контроля качества освоения дисциплины

Контроль качества освоения студентами дисциплины осуществляется с использованием балльно-рейтинговой системы (БРС), являющейся обязательной к использованию всеми структурными подразделениями университета.

Для оценки качества усвоения курса используются следующие формы контроля:

– *текущий:* контроль выполнения практических, аудиторных и домашних заданий;

– *рубежный***:** использование педагогических тестовых материалов для аудиторного контроля теоретических знаний (примеры тестовых заданий в приложении А); учет суммарных результатов по итогам текущего контроля за соответствующий период и систематичность работы; осуществляется в два этапа;

– *семестровый:* осуществляется посредством зачета и суммарных баллов за весь период изучения дисциплины.

Оценка качества освоения дисциплины осуществляется в соответствии с Положением «Об организации учебного процесса по основным образовательным программам высшего профессионального образования» и с Положением «О фонде оценочных средств».

6.2. Виды и перечни заданий для СРС

Темы и формы практических занятий:

№	*№ темы*	*Наименование практического занятия*	*Форма проведения*	*Кол-во баллов*
ПЗ-1	1.2	Основы информационной безопасности и защиты информации – ПЗ-1	Проблемный семинар	3 б.
ПЗ-2	1.3	Классификация информационных ресурсов – ПЗ-2	Проблемный семинар, работа в малой группе	3 б.
ПЗ-3	1.5	Правовое регулирование открытых информационных ресурсов – ПЗ-3	Анализ источников	3 б.
ПЗ-4	1.6.	Правовая защита информационных ресурсов ограниченного доступа - ПЗ-4	Анализ источников	3 б.
ПЗ-5	1.8	Методологические основы системы безопасности предприятия (фирмы) – ПЗ-5	Семинар-обсуждение конкретных ситуаций	3 б.
ПЗ-6	1.9	Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов – ПЗ-6	Проблемный семинар-дискуссия	3 б.
ПЗ-7	1.11.1	Особенности подбора персонала для работы с конфиденциальной информацией – ПЗ-7	Проблемный семинар	2 б.
ПЗ-8	1.11.2	Доступ персонала к конфиденциальным сведениям, документам и базам данных. Организация работы с персоналом, обладающим конфиденциальной	Проблемный семинар	2 б.

		информацией.- ПЗ-8		
ПЗ-9	1.12.2.	Технологические системы защиты и обработки конфиденциальных документов.- ПЗ-9	Проблемный семинар с выполнением практических заданий	3 б.
ПЗ-10	1.12.3.	Принципы учета конфиденциальных документов. Технология обработки подготовленных конфиденциальных документов. - ПЗ-10	Проблемный семинар	3 б.
ПЗ-11	1.13	Инженерно-техническая защита - ПЗ-11	Проблемный семинар	3 б.
ПЗ-12	1.14	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи – ПЗ-12	Семинар-обсуждение	3 б.

Темы домашних заданий для СРС:

№	*№ темы*	Наименование домашнего задания	*Кол-во баллов*
ДЗ-1	Раздел 1	Анализ нормативно-правовых актов	4 б.
ДЗ-2	Раздел 2	Составление сравнительной таблицы	4 б.
ДЗ-3	Раздел 3	Письменный анализ способов защиты информации	4 б.
ДЗ-4	Раздел 4	Подготовка реферата	4 б.

6.3. Зачет

Зачет проводится посредством суммарных баллов за весь период изучения дисциплины (вопросы для самоконтроля приведены в Приложении 1).

6.4. Критерии оценки качества и технологическая карта

Технологическая карта дисциплины с оценкой различных видов учебной деятельности по этапам контроля приведена в приложении № 3.

Критерии оценки качества освоения студентами дисциплины:

- пороговый («оценка «удовлетворительно») – 50 – 69 баллов.
- стандартный (оценка «хорошо») – 70 – 89 баллов.
- эталонный (оценка «отлично») – 90 – 100 баллов.

Критерий	*В рамках формируемых компетенций студент демонстрирует*
пороговый	знание и понимание теоретического содержания курса с незначительными пробелами; несформированность некоторых практических умений при применении знаний в конкретных ситуациях, низкое качество выполнения учебных заданий (не выполнены, либо оценены числом баллов, близким к минимальному); низкий уровень мотивации учения;
стандартный	полное знание и понимание теоретического содержания курса, без пробелов; недостаточная сформированность некоторых практических умений при применении знаний в конкретных ситуациях; достаточное качество выполнения всех предусмотренных программой обучения учебных заданий; средний уровень мотивации учения;

эталонный	полное знание и понимание теоретического содержания курса, без пробелов; сформированность необходимых практических умений при применении знаний в конкретных ситуациях, высокое качество выполнения всех предусмотренных программой обучения учебных заданий (оценены числом баллов, близким к максимальному); высокий уровень мотивации учения.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература:

1. Куняев, Н. Н. Конфиденциальное делопроизводство и защищенный электронный документооборот : учеб. для вузов / Н. Н. Куняев, А. С. Дёмушкин, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - М. : Логос, 2011. - 449, [1] с.
2. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М. : Академия, 2006. - 330, [1] с.
3. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 5-е изд., стер. - М. : Академия, 2011. - 330, [1] с.
4. Мельников, В. П. Защита информации: учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014. – 295 с.
5. Хлебников, А. А. Информационные технологии : учеб. для вузов / А. А. Хлебников. - М. : Кнорус, 2014. - 462, [4] с.
6. Бардаев, Э. А. Документоведение : учебник : для вузов / Э. А. Бардаев, В.Б.Кравченко. - 3-е изд., перераб. и доп. - М. : Академия, 2013. - 332, [2] с.

7.2. Дополнительная литература:

1. Алябьева, О. Организация процесса адаптации // Кадровые решения. – 2007. - №6. - С. 81-86.
2. Аминов, В.Л. Кадровая безопасность предприятия // Кадровые решения. – 2009. – № 10. – С.91-99.
3. Басаков, М.И. От приёма на работу до увольнения (оформление документации в соответствии с новым Трудовым кодексом): Практическое пособие. – 2-е изд., испр. и доп. – Москва: ИКЦ «МарТ», Ростов н/Д: Издательский центр «МарТ», 2005. – 224 с. (Серия «Безупречные документы»)
4. Бахарева, Е.В. Коммерческая тайна // Секретарь-референт. – 2006. – № 11. – С. 43-50.
5. Громыко, И.А. Общая парадигма защиты информации. Определение терминов: от носителей к каналам утечки информации // Защита информации. Инсайд. – 2008. - № 1. – С.12-15.
6. Доля, А.А. Внутренние ИТ-угрозы в России – 2006 // Защита информации. Инсайд. – 2007. - № 2. – С.60-69.
7. Дуракова, И.Б., Родин, О.А., Талтынов, С.М. Управление персоналом: учебное пособие. – Воронеж: Изд-во Воронежского гос. ун-та, 2004. – 82 с.
8. Зенин, Н. Обеспечение конфиденциальности информации – это всегда комплексный подход // Трудовое право. – 2010. – № 1. – С. 41-42.
9. Камаев, В.А., Натров, В.В. Моделирование и анализ состояния информационной безопасности организации // Защита информации. Инсайд. – 2009. - № 4. – С.16-20.
10. Копылов, В.А. Информационное право: учебник / В.А. Копылов ; Московская гос. юрид. акад. – Изд. 2-е, перераб. и доп. - М.: Юристъ, 2005. - 510 с.
11. Корнеев К.И., Степанов Е.А. Защита информации в офисе: учеб. – М.:ТК Велби, Изд-во Проспект, 2008. – 336 с.

12. Мельников, В.П. Информационная безопасность и защита информации : учеб. пособие для студ. высш. учеб. заведений / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. – 3-е изд., стер. – М.: Издательский центр «Академия», 2008. – 336 с.
13. Менеджмент организации / Под ред. З.П. Румянцевой, Н.А. Саламатина. – М.: ИНФРА, 1995. – 188 с.
14. Методы и средства защиты информации: учебное пособие / Под ред. Л.И. Абросимова, А.Ю. Кораблёва. – М.: ИНФРА, 2003. – 56 с.
15. Некраха,А.В. Организация конфиденциального делопроизводства и защиты информации: учебное пособие/ А.В. Некраха, Г.А.Шевцова. – М: Академический проект, 2007. – 224 с.
16. Суханова, И.М. Аттестация и комплексная оценка персонала // Кадровые решения. – 2007. - № 4. – С.76-84.
17. Управление персоналом: Учебник для вузов / Под ред. Т.Ю. Базарова, Б.Л. Ерёмина. – 2-е издание перераб. и доп. – М.: ЮНИТИ, 2002. – 423 с.
18. Чуковенков, А.Ю. Документы по аттестации служащих // Секретарь-референт. – 2006. - № 11. – С. 17-23.
19. Шубин, А.С. Наша Тайна громко плачет… // Защита информации. Инсайд. – 2008. - № 1. С. 19-27.
20. Янковая, В.Ф. Гриф ограничения доступа к документу // Секретарь-референт. – 2008. - № 1. – С. 17-19.
21. Янковая, В.Ф. Организация конфиденциального делопроизводства // Секретарь-референт. – 2009. - № 12. – С.17 – 20.
22. Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.

7.3. Нормативно-правовые источники:

Конституция Российской Федерации // Российская газета. 1993. 25 дек.

О средствах массовой информации. Закон Российской Федерации от 27.12. 1991 № 2124-1// Ведомости съезда народных депутатов РФ и Верховного Совета РФ. - 1992 . - №7. - С. 378 - 399.

Закон Российской Федерации «О безопасности» от 05.03.92 г. // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 15. Ст. 769.

Закон Российской Федерации «О федеральных органах правительственной связи и информации» от 19.02.93 г. №4524-1// Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации.1993. №12. Ст.423.

Федеральный закон «О библиотечном деле» от 29.12.94 г. № 78-ФЗ // Собрание законодательства Российской Федерации. 1995. № 1. Ст. 2.

Федеральный закон «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания» от 14.06.94 г. № 5-ФЗ // Собрание законодательства Российской Федерации. 1994. № 8. Ст. 801.

Федеральный закон «О федеральной фельдъегерской связи» от 17.12.94 г. № 67-ФЗ // Собрание законодательства Российской Федерации. № 34. Ст. 3547.

Федеральный закон «Об обязательном экземпляре документов» от 29.12.94 г. № 77-ФЗ // Собрание законодательства Российской Федерации. 1995. № 1. Ст. 1.

Федеральный закон «О рекламе» от 18.07.95 г. № 108-ФЗ // Собрание законодательства Российской Федерации. №30. Ст. 2864.

Федеральный закон «О порядке освещения деятельности органов государственной власти в государственных органах массовой информации» от 13.01.95 г. № 7-ФЗ // Собрание законодательства Российской Федерации. № 3. Ст. 170.

Федеральный закон «О почтовой связи» от 09.08.95 г. № 129-ФЗ // Собрание законодательства Российской Федерации. № 33. Ст. 3334.

Закон Российской Федерации «О государственной тайне» от 21.07.93 г. с изменениями и дополнениями от 06.10.97 г. // Собрание законодательства Российской Федерации. 1997. № 41. Ст. 4673.

Федеральный закон «О связи» от 16.02.95 г. № 15-ФЗ // Собрание законодательства Российской Федерации.1995. №8. № Ст. 600.

Федеральный закон «Об основах государственной службы Российской Федерации» от 31.07.95 г. № 119-ФЗ // Собрание законодательства Российской Федерации. № 31. Ст. 2990.

Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.95 г. № 144-ФЗ// Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

Федеральный закон «Об электронной цифровой подписи» от 10.01.02 г. №1-ФЗ // Собрание законодательства Российской Федерации. 2002. № 2. Ст. 127.

Федеральный закон «О коммерческой тайне» от 09.07.04 г. №98-ФЗ // Собрание законодательства Российской Федерации. 2004. № 32. Ст.3283.

Федеральный закон РФ «Об архивном деле в Российской Федерации» от 22 .10. 2004 . // Собрание Законодательства Российской Федерации. 2004. № 43. Ст. 4169.

Федеральный Закон от 13.03. 2006 . № 38–ФЗ «О рекламе» // Собрание Законодательства Российской Федерации. 2006. № 12. Ст. 1232.

Федеральный Закон от 27.07. 2006 . № 149–ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание Законодательства Российской Федерации. 2006. № 31. (Ч. 1). Ст. 3448.

Федеральный Закон от 27.07. 2006 . № 152–ФЗ «О персональных данных» // Собрание Законодательства Российской Федерации. 2006. № 31. (Ч. 1). Ст. 3451.

Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред.13.05.2008) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001. № 195-ФЗ (ред.16.05.2008) // Собрание законодательства Российской Федерации. 2002. № 1. (Ч.1). Ст. 1.

Трудовой Кодекс Российской Федерации об от 30.12.2001. № 197-ФЗ (ред.28.02.2008) // Собрание законодательства Российской Федерации. 2002. № 1. (Ч.1). Ст. 3.

Гражданский кодекс Российской Федерации. Часть четвертая от18.12.2006 № 230-ФЗ // Собрание законодательства Российской Федерации. 2006. № 52. Ст. 1232.

Указ Президента Российской Федерации «Об основах государственной политики в сфере информатизации» от 20.01.94 г. № 170 // Собрание актов Президента и Правительства Российской Федерации. 1994. № 4. Ст. 305.

Указ Президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне» от 30.11.95 г. №1203; в редакции Указа Президента РФ от 24.01.98№ 61 от 06.06.01 г. №659 // Собрание законодательства Российской Федерации. 1998. №5. Ст.561; 2001. №24. Ст.2418.

«Положение о Межведомственной комиссии по защите государственной тайны» утверждено Указом Президента Российской Федерации от 20.01.96 г. №71 // Собрание законодательства Российской Федерации. 1996. № 4. Ст. 268.

Указ Президента Российской Федерации «О концепции национальной безопасности Российской Федерации» от 10.01.2000 г. № 24 // Собрание законодательства Российской Федерации. 2000. № 2. Ст. 170.

«Доктрина информационной безопасности Российской Федерации» утверждена Указом Президента Российской Федерации 09.09.00 г. №ПР-1895 // Российская газета №187 от 28.09.00 г.

Указ Президента Российской Федерации «О концепции национальной безопасности Российской Федерации» от 10.01.2000 г. № 24 // Собрание законодательства Российской Федерации. 2000. № 2. Ст. 170.

Постановление Правительства Российской Федерации «Правила отнесения сведений составляющих государственную тайну, к различным степеням секретности» от 04.09.95 г. № 870 // Собрание законодательства Российской Федерации. 1995. № 37. Ст. 3619.

Постановление Правительства Российской Федерации «О государственном учете и регистрации баз и банков данных» от 28.02.99 г. № 226 // Собрание законодательства Российской Федерации. 1999 №12. Ст.1114.

ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, созданным средствами вычислительной техники. М.: Изд-во Стандартов, 1985.

ГОСТ 6.10.1-88. Унифицированные системы документации. Основные положения. М.: Изд-во Стандартов, 1988.

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. М., 1990.

ГОСТ Р-22.0.04-95. Безопасность в чрезвычайных ситуациях. Биолого-социальные чрезвычайные ситуации. Термины и определения. М., 1995.

ГОСТ Р-22.3.05-96. Безопасность в чрезвычайных ситуациях. Жизнеобеспечение населения в чрезвычайных ситуациях. Термины и определения. М.: Изд-во Стандартов, 1996.

ГОСТ Р 50922-96. Защита информации: Основные термины и определения. М., 1996.

ГОСТ Р 6.30-97. Унифицированные системы документации: Система организации норм распорядительной документации: Требования к оформлению документов. М.: Госстандарт. 1998.

ГОСТ 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования и методы испытания. М.: Изд-во Стандартов, 1999.

ГОСТ 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М., 2000.

ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов. М.: Госстандарт, 2003.

Основные правила работы ведомственных архивов. М., 1988.

7.4. Электронные ресурсы:

Справочно-поисковые системы информационно-правового обеспечения ГАРАНТ-Максимум и КОНСУЛЬТАНТ +

1. Центр проблем информационного права - http://www.medialaw.ru/
2. Институт развития информационного общества в России http://www.iis.ru/index.html

Карта учебно-методического обеспечения по дисциплине представлена в приложении № 4.

8. Материально-техническое обеспечение дисциплины

Для осуществления образовательного процесса по дисциплине необходим компьютерный класс, оборудованный мультимедийными средствами для демонстрации лекций-презентаций и презентаций сообщений, индивидуальных заданий.

Приложения

Приложение № 1
Вопросы для самоконтроля по дисциплине «Информационная безопасность и защита информации»

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного доступа к информации.
13. Охарактеризовать технические каналы несанкционированного доступа к информации.
14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.
15. Проанализировать особенности угроз автоматизированным информационным системам.
16. Дать классификацию удаленных атак.
17. Проанализировать основные направления правовой защиты информации.
18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.
19. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.
20. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.
21. Определить объекты защиты авторских прав.
22. Назвать основные права автора в отношении его произведения.
23. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.
24. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).
25. Дать определение государственной тайны и назвать грифы секретности.
26. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
27. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.
28. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.

29. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.
30. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.
31. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.
32. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.
33. Назвать основные положения концепции информационной безопасности предприятия.
34. Изложить содержание регламента обеспечения информационной безопасности предприятия.
35. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.
36. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.
37. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
38. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.
39. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.
40. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.
41. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.
42. Проанализировать особенности текста конфиденциального документа.
43. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.
44. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.
45. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.
46. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.
47. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.
48. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.
49. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.
50. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.
51. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией. .
52. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.
53. Составить схему каналов возможной утраты конфиденциальной информации,

находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.

54. Назвать основные элементы физической защиты территории и помещений предприятия.
55. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.
56. Дать классификацию компьютерных вирусов.
57. Описать основные антивирусные программы.
58. Охарактеризовать основные способы криптографического преобразования данных.

Приложение № 2

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
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 секретаря-референта небольшой 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.

Приложение № 3

Технологическая карта дисциплины
Трудоемкость дисциплины 2 ЗЕ = 50 б.*2=100 баллов (6 семестр)

Семестр, неделя	Аудиторный контроль теоретических знаний (в баллах)	Работа на практических занятиях (в баллах)	Домашние практические задания. (в баллах)	Оценка по итогам работы студента в семестре (в баллах)	Творческий рейтинг	Зачет (в баллах)
1 сем	**1 этап**					
1						
2		ПЗ-1.2 (3)				
3		ПЗ-1.3(3)				
4			ДЗ-1 (4)			
5		ПЗ-1.5 (3)				
6		ПЗ-1.6 (3)				
7			ДЗ-2 (4)			
8		ПЗ-1.8 (3)				
9	Контрольная работа (20)	ПЗ-1.9 (3)				
	0-20	0-18	0-8	0-4		
	1 этап: рубежная аттестация (не менее 25 из 50 баллов)					
	2 этап					
10						
11		ПЗ-1.11.1 (2)				
12		ПЗ-1.11.2 (2)				
13			ДЗ-3 (4)			
14		ПЗ-1.12.2 (3)				
15		ПЗ-1.12.3 (3)				
16			ДЗ-4 (4)			
17		ПЗ-1.13 (3)				
18	Контрольная работа (20)	ПЗ-1.14 (3)				
	0-20	0-16	0-8	0-4	0-2	
2 этап: рубежная аттестация (не менее 25 из 50 баллов)						
	0-40	0-34	0-16	0-8	0-2	
	СЕМЕСТРОВАЯ АТТЕСТАЦИЯ (не менее 50 баллов из 100)					

Критерии оценки качества освоения студентами дисциплины:
- пороговый («оценка «удовлетворительно) – 50 – 69 баллов.
- стандартный (оценка «хорошо») – 70 – 89 баллов.
- эталонный (оценка «отлично») – 90 – 100 баллов.

Приложение № 4

Карта учебно-методического обеспечения

Дисциплины «Информационная безопасность и защита информации», формы обучения – очной.
Всего часов – 36, из них:
- лекций – 12, практических занятий – 24, СРС ауд. – 12,
- СРС внеауд. – 36
- зачет;
Для направления 034700.62 - «Документоведение и архивоведение».
Выпускающая кафедра – «Истории России и архивоведения», семестр 6

Таблица 1 – Обеспечение дисциплины учебными изданиями

Библиографическое описание издания (автор, наименование, вид, место и год издания, к-во стр.)	Вид занятия	К-во экз. в в-ке НовГУ	ЭБС	Примечание
Куняев, Н. Н. Конфиденциальное делопроизводство и защищенный электронный документооборот : учеб. для вузов / Н. Н. Куняев, А. С. Дёмушкин, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - М. : Логос, 2011. - 449, [1] с.	Лекция, ПЗ, СРС	12		
Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М. : Академия, 2006. - 330, [1] с.	Лекция, ПЗ, СРС	4		
Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 5-е изд., стер. - М. : Академия, 2011. - 330, [1] с.	Лекция, ПЗ, СРС	2		
Мельников, В. П. Защита информации : учебник : для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014. - 295, [2] с.	Лекция, ПЗ, СРС	2		
Хлебников, А. А. Информационные технологии : учеб. для вузов / А. А. Хлебников. - М. : Кнорус, 2014. - 462, [4] с.	Лекция, ПЗ, СРС	3		
Бардаев, Э. А. Документоведение : учебник : для вузов / Э. А. Бардаев, В. Б. Кравченко. - 3-е изд., перераб. и доп. - М. : Академия, 2013. - 332, [2] с.	Лекция, ПЗ, СРС	2		

Таблица 2 – Обеспечение дисциплины учебно-методическими изданиями

Библиографическое описание издания (автор, наименование, вид, место и год издания, к-во стр.)	Вид занятия	К-во экз. в б-ке НовГУ	ЭБС	Примечание
Арутюнов, В. В. Защита информации : учеб.-метод. пособие. - М. : Либерея-Бибинформ, 2008. - 55,[1]с.	ПЗ, СРС	1		
Рабочая программа дисциплины «Информационная безопасность и защита информации»	ПЗ, СРС			www.novsu.ru/dept/20353816 документы

Действительно для учебного года 2014/2015

Зав. кафедрой _____ _____
подпись И.О.Фамилия
_____ _____ 20….. г.

СОГЛАСОВАНО:

НБ НовГУ: _____ _____ _____
должность подпись расшифровка

Приложение 5
Лист внесения изменений

Номер изменения	Номер и дата распорядительного документа о внесении изменений	Дата внесения изменения	ФИО лица, внесшего изменение
№1			
№2			
№3			