

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

УТВЕРЖДАЮ

Декан факультета

 Л.Р. Фионова


«31» июля 2015 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ЗАЩИТА
ИНФОРМАЦИИ
(Б1.1.21)**

Направление подготовки 46.03.02 Документоведение и архивоведение

Профиль подготовки документационное обеспечение управления

Квалификация (степень) выпускника бакалавр

Форма обучения очная

Пенза 2015

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины модуля Б1.1.22 «Конфиденциальное делопроизводство и защита информации» являются – формирование компетенций по технологиям эффективной защиты экономических интересов организаций, органов государственного и местного самоуправления, реализующей механизмы конфиденциального делопроизводства с учетом требований нормативно-правовых документов, регламентирующих защиту конфиденциальных сведений и ведения делопроизводства и выполнение на нормативно-правовой основе требований по информационной безопасности и защите информации.

Задачи:

- 1) ведение конфиденциального делопроизводства;
- 2) обеспечение контроля над режимом конфиденциальности;
- 3) организация и ведение электронного конфиденциального делопроизводства;
- 4) внесение обоснованных предложений руководству предприятия (учреждения) по вопросам; организации и совершенствования конфиденциального делопроизводства;
- 5) изучение направлений и нормативно-методических документов по информационной безопасности и защите информации;
- 6) изучение методов, форм и средств организационной защиты информации;
- 7) изучение технологии выполнения работ по информационной безопасности и защите информации;
- 8) изучение методов, форм и средств технической защиты информации;
- 9) изучение угроз информационной безопасности на объектах информатизации и применение специализированных аппаратных и программных средств по защите информации;
- 10) воспитание культуры работы с документированной информацией, требующей защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОИ БАКАЛАВРИАТА :

Дисциплина относится к блоку базовых дисциплин, ведется в 5 семестре и базируется на входных знаниях по следующим дисциплинам:

–Б1.1.7. «Правовое обеспечение профессиональной деятельности» (2 семестр; ОК-4; ПК-33);

– Б1.1.10 «Информационные технологии в профессиональной деятельности» (1 семестр; ОК-10; ОПК-2);

– Б2.1 «Практика по документоведению» (2 семестр; ОК-5; ОК-6; ОК-7; ОК-10; ОПК-1; ОПК-4; ОПК-6; ПК-1; ПК-2; ПК-4; ПК-11; ПК-14; ПК-15; ПК-16; ПК-20; ПК-25; ПК-29; ПК-33; ПК-34; ПК-35;);

– Б2.2 «Практика по технологии документационного обеспечения управления» (4 семестр; ОК-5; ОК-6; ОК-7; ОК-10; ОПК-1; ОПК-4; ОПК-6; ПК-2; ПК-4; ПК-11; ПК-14; ПК-15; ПК-16; ПК-20; ПК-25; ПК-29; ПК-30; ПК-32; ПК-33; ПК-34).

Студенты должны обладать умением аналитической деятельности, работе с нормативно-методическими документами, знать юридические основы в документоведении и архивоведении. Предшествующей дисциплиной является документоведение.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ Б1.1.22 «КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ЗАЩИТА ИНФОРМАЦИИ»

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Коды компетенции	Наименование компетенции	Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть)
1	2	3
ОПК-6	<p>Общекультурной компетенцией:</p> <p>– способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>	<p>Знать: Основные понятия в области информационной безопасности при работе в информационных сетях при осуществлении профессиональной деятельности, знать основы конфиденциального делопроизводства.</p> <p>Уметь: пользоваться информационными технологиями ДООУ с учетом требований информационной безопасности</p> <p>Владеть: решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности</p>
ПК-17	<p>Профессиональной компетенцией:</p> <p>в технологической деятельности:</p> <p>– владением методами защиты информации</p>	<p>Знать: основные технологические этапы защиты информации в системе документооборота.</p> <p>Уметь: идентифицировать основные угрозы информационной безопасности в конфиденциальном документообороте.</p> <p>Владеть: навыками защиты информации в профессиональной деятельности, методами работы с конфиденциальными и секретными документами.</p>
ПК-38	<p>В организационно-управленческой деятельности:</p> <p>– владением навыками работы с документами, содержащими информацию ограниченного доступа</p>	<p>Знать: основные нормативные документы при осуществлении конфиденциального документооборота.</p> <p>Уметь: работать с документами, содержащими конфиденциальную информацию.</p> <p>Владеть: навыками работы с документами, содержащими информацию ограниченного доступа</p>

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ Б1.1.22 «КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ЗАЩИТА ИНФОРМАЦИИ»

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 144 часов.

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)									Формы текущего контроля успеваемости (по неделям семестра)							
				Аудиторная работа				Самостоятельная работа					Собеседование	Коллоквиум	Проверка тестов	Проверка контрол. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект)	др.
				Всего	Лекция	Практические занятия	Лабораторные занятия	Всего	Подготовка к аудиторным занятиям	Реферат, эссе и др.	Курсовая работа (проект)	Подготовка к экзамену								
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1.	Раздел 1. Профессиональная деятельность на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-6);	5	1-5	18	10		8	22	12		10		9-15						2-5	
1.1.	Раздел 2 Методы защиты информации (ПК-17).	5	6-12	26	14		12	24	14		10		9-15						7-12	
1.2.	Раздел 3 Работа с документами, содержащими информацию ограниченного доступа (ПК-38)	5	13-18	28	12		16	26	14		12		9-15						13-18	
	<i>Курсовая работа (проект)</i>																			
	<i>Подготовка к экзамену</i>											36								

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
	Общая трудоемкость, в часах			72	36		36	72	40		32		Промежуточная аттестация							
													Форма				Семестр			
													Зачет				<i>нет</i>			
													Экзамен				5			

4.2. Содержание дисциплины (модуля)

- | • Наименование раздела дисциплины | • Содержание раздела |
|---|--|
| 1. Профессиональная деятельность на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-6); | • Понятие информации, свойства защищаемой информации, комплексный подход; понятие целей информационной защиты; критерии защиты. |
| 1.1 Понятие защищаемой информации и комплексного подхода к организации защиты. | • Структура системы защиты, совокупность организационно-технических мероприятий, основные этапы информационной защиты. |
| 1.2 Концепция информационной безопасности организации. | • Информационный риск. Нормирование риска информационных угроз |
| 1.3 Критерии управления информационной безопасностью организации. | |
| • 2. Методы защиты информации (ПК-17). | • Структурирование защищаемой информации, организация работа с секретными документами. |
| 1.4 Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации. | • Порядок допуска сотрудников с сведениям, составляющих гос. и коммерческую тайны; ограничения на допуск сотрудников к конфиденциальной информации. Документирование допуска сотрудников к государственной и коммерческой тайне. |
| 1.5 Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну | • Мониторинг информационной безопасности; основные угрозы информационной безопасности со стороны персонала; мониторинг лояльности персонала; организация обучения; методы тренинга персонала с использованием информационных технологий. |
| 1.6 Определение категорий сотрудников и подбор персонала для работы с конфиденциальной информацией | • Основные источники риска информационной безопасности при проведении презентаций, конференций и выставок; перечень и состав необходимых мероприятий по профилактике информационных угроз. |
| 1.7 Оформление допуска сотрудников к конфиденциальной информации | • Основные источники риска информационной безопасности при работе с посетителями; требования к организации офиса; понятие закладных устройств; технические средства наблюдения. |
| 1.8 Текущая работа с персоналом и обучение сотрудников правилам и приемам работы с конфиденциальной информацией | • Обеспечение информационной безопасности при осуществлении контактов с зарубежными партнерами; технические средства разведки. |
| 1.9 Организация пропускного и внутриобъектового режимов | • Основные источники угроз информационной безопасности при проведении выставок; основные легальные методы получения конфиденциальной информации. |
| 1.10 Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам | • Организация работы экспертных групп. |
| 1.11 Организация защиты информации при приеме в организации посетителей | • Перечень сведений, составляющих государственную тайну, основные нормативные документы, регламентирующие порядок допуска сведений к открытому опубликованию; ответственность авторов публикаций. |
| 1.12 Организация защиты конфиденциальной информации при осуществлении международного сотрудничества | • Алгоритм создания защиты; организация разрешительной системы доступа к конфиденциальной информации; организация физической охраны организации. |
| 1.13 Организация защиты информации при осуществлении рекламной и выставочной деятельности | • Вещественные каналы возможной утечки конфиденциальной информации. Классификация каналов по уровню угроз информационной безопасности. |
| 1.14 Организация защиты информации при подготовке материалов к открытому опубликованию | |
| 1.15 Организация защиты конфиденциальной продукции в процессе ее изготовления, хранения и транспортировки. Система комплексной защиты конфиденциальной информации. | |
| 1.16 Выделение помещений для работы с конфиденциальными документами, изделиями, проведения работ. | |
| 1.17 Анализ возможных угроз безопасности конфиденциальной информации при использовании | |

технических средств управления.

1.18 Меры и средства технической защиты конфиденциальной информации, обрабатываемой техническими средствами.

3 Работа с документами, содержащими информацию ограниченного доступа (ПК-38)

1.19 Понятие и особенности конфиденциального делопроизводства.

3.2 Нормативная база конфиденциального делопроизводства. Служебная и коммерческая тайна. Другая информация ограниченного доступа

3.3 . Организационные службы конфиденциального делопроизводства. Понятие и принципы организации конфиденциального делопроизводства

3.4 Создание и учет конфиденциальных документов, порядок обращения с конфиденциальными документами

- Роль и место конфиденциального делопроизводства в обеспечении защиты конфиденциальной информации Конфиденциальное делопроизводство как составная часть управленческой деятельности. Конфиденциальное делопроизводство и открытое делопроизводство.

- Законодательные и иные нормативные правовые акты в сфере информационной безопасности и организации работы с документами ограниченного доступа. Локальные нормативные акты организации по организации работы с документами ограниченного доступа.

- Положение о подразделении конфиденциального делопроизводства. Штатный состав и численность подразделения конфиденциального делопроизводства. Должностные инструкции работников. Особенности трудовых отношений с работниками подразделения конфиденциального делопроизводства.

- Схема прохождения документа при создании, регистрации и визировании, передача конфиденциальных документов внутри организации.

- Порядок вноса-выноса документов, содержащих конфиденциальные сведения и работы на рабочем месте с конфиденциальной информацией.

- Схема прохождения входящих и исходящих конфиденциальных документов.

- Организация учета лиц, получивших доступ к информации, составляющей коммерческую тайну или содержащую иные конфиденциальные сведения, и (или) лиц, которым такая информация была предоставлена или передана.

- Подготовка к заключению договоров с контрагентами, задачи по соблюдению конфиденциальности.

- Типовые формы Соглашений о конфиденциальности.

- Порядок передачи сведений (ознакомления со сведениями), составляющих коммерческую тайну, и других конфиденциальных сведений органам государственной власти и местного самоуправления.

- Порядок размножения и снятия копий с конфиденциальных документов.

- Контроль исполнения конфиденциальных документов.

- Порядок действий при необходимости использования конфиденциальных документов в командах.

4.3 Лабораторный практикум

	№ раздела дисциплины	Наименование лабораторных работ	Трудоемкость (час.)
	<p>1. Профессиональная деятельность на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-6);</p> <p>2. Методы защиты информации (ПК-17).</p>	<p>№1 Моделирование угроз безопасности информации.</p> <p>№2 Разработка моделей объектов информационной защиты</p> <p>№3 Анализ рисков информационных угроз.</p> <p>№4 Разработка плана эшелонированной защиты предприятия от информационных угроз с применение зонального принципа.</p> <p>№5 Выбор технических средств защиты объекта от информационных угроз.</p>	<p>4</p> <p>2</p> <p>4</p> <p>4</p> <p>4</p>
	<p>3 Работа с документами, содержащими информацию ограниченного доступа (ПК-38)</p>	<p>№6. Разработка «Инструкции по конфиденциальному делопроизводству».</p> <p>№7. Подготовка и оформление документов с грифами конфиденциальности.</p> <p>№8. Учет и регистрация документов с грифами конфиденциальности.</p> <p>№9. Передача и отправка документов с грифами конфиденциальности.</p> <p>№10. Копирование (тиражирование) документов с грифами конфиденциальности.</p> <p>№11. Группировка документов с грифами конфиденциальности в дела.</p> <p>№12. Уничтожение документов с грифами конфиденциальности.</p> <p>№13. Контроль состояния конфиденциального делопроизводства.</p>	<p>2</p> <p>2</p> <p>2</p> <p>2</p> <p>2</p> <p>2</p> <p>2</p> <p>4</p>
Всего часов			36

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Таблица 5.1

П/п	Вид образовательной технологии	Раздел I	Раздел II	Раздел III	Самостоятельная работа
5.1	Электронные пособия. (Авторский электронный учебник «Информационная безопасность и защита информации»)	Темы 2.1–2.15			Курсовая работа Подготовка к лекциям. Подготовка к лабораторным работам.
5.2	Мультимедийные лекции (Авторский цикл из трех модулей «Защита и обработка конфиденциальных документов»)	Тема 1.1	Темы 2.1; 2.2	Темы 3.1; 3.2	Курсовая работа Подготовка к лекциям. Подготовка к лабораторным работам
5.3	Наглядные пособия и стенды по техническим средствам защиты информации в офисах и архивах.	Тема 1.1	Темы: 2.3–2.5	Тема 3.3	Курсовая работа Подготовка к лекциям. Подготовка к лабораторным работам
5.4	Экскурсии на объекты информационной инфраструктуры региона (Правительство Пензенской области, ООО Арсенал+)	Тема 1.1 Тема 3.2		Тема 3.3	Подготовка к лекциям. Подготовка к лабораторным работам
5.5	Деловые игры с разбором вероятных событий риска информационных угроз в конфиденциальном документообороте и способов их профилактики.	Лабораторный практикум: работы 1–3	Лабораторный практикум: работа 4	Лабораторный практикум: работы 6–13	Курсовая работа Подготовка к лекциям. Подготовка к лабораторным работам
5.6	Факультативные беседы разработчиков технических средств защиты информации, систем защиты объектов (знакомство с продукцией ФГУП НПО «НИКИРЭТ», ЦЕСИС)	Все темы	Все темы	Все темы	Подготовка к лекциям. Подготовка к лабораторным работам
5.7	Работа с правовой системой Консультант Плюс.	Темы 1.1; 1.2	Тема 2.12	Тема 3.2	Нормативное правовое обеспечение курсовой работы.
5.8	В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по собственной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы со студентами, в том числе в электронной образовательной среде с использованием соответствующего программного обеспечения, дистанционных форм обучения, возможностей Интернет-ресурсов, индивидуальных консультаций и т.д.				

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
2 3 4 5	1.1. Понятие целей информационной защиты; критерии защиты 1.2. Структура системы защиты. 1.3. Основные этапы информационной защиты.	Образовательные технологии: 5.2; 5.3 Работа над КР. Подготовка к лекциям. Подготовка к лабораторным работам.	Разработать структурную схему организации в соответствии с заданием на КР. Предложить этапы защиты.	[1, 12]	22
6 7 8 9 10 11 12	2.3 Порядок допуска сотрудников с сведениям, составляющих гос. и коммерческую тайны. 2.13–2.16 -Организация работы экспертных групп. -Перечень сведений, составляющих государственную тайну. -Основные нормативные документы, регламентирующие порядок допуска сведений к открытому опубликованию. --- Организация физической охраны организации. -Вещественные каналы возможной утечки конфиденциальной информации.	Образовательные технологии: 5.3; 5.7. Выполнение плана работы над КР. Подготовка к лекциям. Подготовка к лабораторным работам	Структурировать защищаемую информацию. Выделить основные источники риска информационной безопасности. Выделить основные вещественные каналы возможной утечки информации. Разработать вариант зональной защиты объекта по легенде КР.	[14, 15, 22, 23]	24

13 14 15 15 17 18	3.1 – 3.4 Законодательные и иные нормативные правовые акты в сфере информационной безопасности и организации работы с документами ограниченного доступа	Образовательные технологии: 5.3; 5.4; 5.7. Выполнение плана работы над КР. Подготовка к лабораторным работам. Подготовка к лекциям.	Разработать Положение о подразделении конфиденциального делопроизводства в рамках задания на КР. Разработать схему прохождения входящих и исходящих конфиденциальных документов	[4, 24, 25]	26
----------------------------------	---	--	--	-------------	----

6.2. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов

6.2.1 Читальный зал университета

6.2.2 Компьютерные классы для самостоятельной работы библиотеки университета.

6.2.3 Самостоятельная работа над заданием по курсовому проектированию проводится студентами со 2 недели до 18 недели и завершается ее защитой. План выполнения курсовой работы контролируется еженедельно по установленному графику.

6.2.4 Подготовка к лекционным занятиям предусматривает самостоятельное изучение дополнительной литературы по дисциплине с текущим контролем в установленные часы консультаций по графику консультаций.

6.2.5 Самостоятельная работа по лабораторному практикуму предусматривает оформление лабораторных работ и теоретическую подготовку к защите работ по графику выполнения в начале следующего по графику лабораторного занятия.

При самостоятельной работе студенты используют переданный методический материал преподавателя в электронной форме, ресурсы библиотечного фонда университета и кафедры.

6.3. Материалы для проведения текущего и промежуточного контроля знаний студентов

Тестовые задания выдаются студентам лектором на в соответствии с графиком промежуточного контроля знаний, предусмотренным УМК.

Для выполнения письменного ответа предусмотрен временной интервал 15-20 минут. Проведение промежуточного контроля знаний проводится в начале лекции письменно.

Оценки ответов производится по 100 бальной шкале. При этом оценка от 60 до 70 баллов признается "удовлетворительно"; - от 71 до 80 баллов - "хорошо"; - от 81 до 100 - "отлично".

При подсчете баллов преподаватель условно разделяет требуемый ответ, состав которого определен лекционным материалом, на пять значимых модулей, каждый из которых оценивается максимум по 20 баллов.

Контроль освоения компетенций

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
6.3.1	Проверка графика выполнения курсовой работы и качества выполнения задания. Раздел 1 КР. Собеседование. Контроль готовности к лабораторным работам и к лекциям по графику выполнения.	1.1 – 1.3	ОПК-6

6.1.2	Контроль готовности к лабораторным работам и к лекциям по графику выполнения. Раздел 2 КР. Собеседование.	2.3; 2.15, 2.16	ОПК-6, ПК-17
6.1.3	Контроль готовности к лабораторным работам и к лекциям по графику выполнения. Раздел 3,4 КР. Собеседование.	3.3 – 3.4	ПК-38

Демонстрационный вариант теста

1. С какой целью на предприятии создается система защиты коммерческой тайны?
2. Какие сведения не могут составлять коммерческую тайну?
3. Какую информацию собственник обычно относит к категории защищаемой?
4. Что понимается под утечкой конфиденциальной информации и, что способствует утечке?
5. Какие основные документы организации определяют отношение сведений к коммерческой тайне?
6. Что является объектом защиты информации, и какие при этом устанавливаются цели?
7. Что включает в себя текущая работа с персоналом, владеющим конфиденциальной информацией?

Собеседование проводится на 9 и 15 неделях семестра в контрольных точках.

Вопросы для собеседования.

1. С какой целью на предприятии создается система защиты коммерческой тайны?
3. Какие сведения не могут составлять коммерческую тайну?
4. Какую информацию собственник обычно относит к категории защищаемой?
5. Что понимается под утечкой конфиденциальной информации и, что способствует утечке?
6. Какие основные документы организации определяют отношение сведений к коммерческой тайне?
7. Что является объектом защиты информации, и какие при этом устанавливаются цели?
8. На каких принципах строится система конфиденциального документооборота
9. Что включает в себя текущая работа с персоналом, владеющим конфиденциальной информацией?

Примерный перечень вопросов и заданий к экзамену

1. Какую информацию относят к защищаемой?
2. Свойства защищаемой информации.
3. Классификация защищаемой информации и ее носителей.
4. Основные нормативные документы по информационной безопасности и защите информации.
5. Принципы засекречивания информации и степени ее секретности.
6. Организационно-правовые формы засекречивания информации, отнесенной к государственной тайне.
7. Цели и задачи системы безопасности предприятия.
8. Характеристика основных каналов возможной утечки защищаемой информации в организациях.
9. Характеристика технических каналов утечки информации.

10. Методы защиты информации в организации от несанкционированного доступа и возможной утечки.
11. Учет конфиденциальных документов в организации.
12. Отдел кадров, текущая работа с персоналом, обладающим конфиденциальной информацией.
13. Роль секретаря-референта в обеспечении информационной безопасности фирмы.
14. Свойства защищаемой информации.
15. Организационные меры защиты информации.
16. Понятие риска информационных угроз.
17. Понятие и принципы организации конфиденциального документооборота.
18. Учет и оформление бумажных носителей конфиденциальной информации.
19. Технологическая система обработки и хранения конфиденциальных документов.
20. Контроль исполнения конфиденциальных документов.
21. Основные принципы отнесения информации к категориям секретной или иной конфиденциальной?
22. Цели и задачи системы информационной безопасности организации.
23. Понятие информационного риска и как он обычно определяется в практике информационной защиты?
24. Каким образом производится присвоение, снятие или изменение грифа секретности или конфиденциальности документов?
25. Классификация и характеристика основных каналов возможной утечки конфиденциальной информации.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ) Б1.1.22 «КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ЗАЩИТА ИНФОРМАЦИИ»

а) основная литература:

1. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. пособие для вузов по спец. "Документоведение и документационное обеспечение управления. ". — М.: ИНФРА-М, 2005. — 301 с. — (Сер.: Высшее образование)
2. Документы и делопроизводство: Справочное пособие /Т.В.Кузнецова, М.Т.Лихачев, А.Л.Райхцаум, А.В.Соколов: Сост. М.Т.Лихачев. – М.: Экономика, 2005, 271 с.
3. Торокин А.А. Основы инженерно-технической защиты информации. - М.: Издательство "Ось-982, 2006 г. - 336 с.
4. Алексенцев А.И. Конфиденциальное делопроизводство. ООО «Журнал «Управление персоналом», 2006. - 200 с.
1. Быкова Т.А., Кузнецова Т.В. Подготовка совещаний и собраний (практическое пособие). – М.: ЗАО «Бизнес-школа «Интел-Синтез», 2008, 76 с.
2. Сердюк В. А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий Издательство: Высшая Школа Экономики (Государственный Университет)
3. ISBN 978-5-7598-0698-1; 2011 г.
4. Организация работы с документами: Учебник / В.А. Кудряев и др. - М.: ИНФРА-М, 2008. 575 с.
5. Информационное обеспечение механизмов управления регионом. - М.: Финансы и статистика, 2005. 128 с.

б) дополнительная литература

6. Никитин Ф.Н. Администратор безопасности корпоративной сети и его инструментарий. //Защита Информации. Конфидент. - 2007. - № 2. - С. 60-65.
7. Теория и практика обеспечения информационной безопасности. / Под ред. П.Д.Зегжды. - М.: Яхтсмен, 2008. - 192 с.
8. Панкратьев В. Организация конфиденциального делопроизводства. На сайте www.Daily.Sec.Ru

9. Печерский А.В., Кирюхин Ю.Г., Тростянский Г.М. Анализ объектов и угроз при защите информации в офисе. (Методические указания к выполнению лабораторных работ) Изд-во Пенз. гос. университета, Пенза, 2010. -32 с.
10. А.В.Печерский. Защищенный документооборот. Метод.указания к курсовому проектированию по дисциплине "Информационная безопасность и защита информации", Изд-во Пенз. ГУ, пенза, 2006.

Законы и Законодательные акты

Приводится перечень только основных нормативных актов в области информационной безопасности.

1. Конституция Российской Федерации.
2. Гражданский кодекс Российской Федерации.
3. Уголовный кодекс Российской Федерации.
4. Уголовно-процессуальный кодекс Российской Федерации.
5. Федеральный закон от 21.07.1993г. №15485-1 «О государственной тайне» (с изменениями, внесенными Федеральным законом от 06.10.2007 года № 131-ФЗ»)
6. Федеральный закон от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и защите информации»
7. Федеральный закон «О коммерческой тайне" от 29 июля 2004 года N 98-ФЗ.
8. Закон РФ "О связи". № 15-ФЗ от 20.01.1995г.
9. Закон РФ № 2446-1 от 5 марта 1992 года. "О безопасности".
10. Закон РФ от 27 декабря 1991 года. "О средствах массовой информации".
11. Федеральный закон № 40-ФЗ от 3 апреля 1995 года.
12. "Об органах Федеральной службы безопасности в Российской Федерации".
13. Закон РФ от 4 июля 1996 года N 85-ФЗ "Об участии в международном информационном обмене".
14. Инструкция о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне. Утверждена постановлением Правительства Российской Федерации от 28 октября 1995 г. № 1050 (с изменениями и дополнениями от 8 августа 2003 г. № 475)
15. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Утверждены постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870
16. "Доктрина Информационной безопасности Российской федерации" от 9 сентября 2000 г. № пр-1895.
17. Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера";
18. Постановление Правительства РФ от 04 сентября 1995г. N 870 "Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности".
19. ГОСТ 3 51275-99 "Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения".
- 20.
21. Копылов В.А. Информационное право: Учебник - 2-е издю, перераб. доп., - М.: Юрист, 2002.-512 с.
22. Гринберг А.С., Горбачев Н.Н., Тепляков А.А. Защита информационных ресурсов государственно-го управления: Учебное пособие для вузов. - М.: ЮНИТА-ДАНА, 2003. 327 с.
23. Информационные технологии в управлении: Учебное пособие/ под ред. Ю.М. Черкасова. - М.: ИНФРА-М, 2001. 216 с.

в) программное обеспечение и Интернет-ресурсы

24. Электронное учебное пособие по основам электронного документооборота и защите информации; / А.В. Печерский. А. С. Гуськов - №15801 ИНИМ РАО ОФЭРНиО, 2010 г.
25. Защищенный документооборот: методические указания / - пенза: Изд-во ПГУ, 2005. Электронная копия ресурса библиотеки федеральных образовательных порталов <http://window.edu.ru/window/library>
26. Комплект презентаций по курсу (выдается преподавателем на электронном носителе каждому студенту).

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
перечень специализированных аудиторий, кабинетов и лабораторий

1. Проведение лекционных занятий

1.1 Лекционные аудитории университета, в том числе. Оснащенные мультимедийными средствами.

2. Проведение лабораторных занятий

2.1 Лабораторные аудитории кафедры ИнОУП, оснащенные средствами вычислительной техники, техническими средствами защиты информации.

3. Самостоятельная работа студентов

3.1 Читальный зал университета

3.2 Компьютерные классы для самостоятельной работы библиотеки университета.

Рабочая программа дисциплины Б1.1.22 «Конфиденциальное делопроизводство и защита информации» составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ПрООП по направлению подготовки бакалавров 46.03.02 «Документоведение и архивоведение».

Программу составили:

А.В. Печерский, профессор

Настоящая программа не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.

Программа одобрена на заседании кафедры «Информационное обеспечение и производства»

Протокол № 1 от «20» июня 2015 года

Зам. зав. кафедрой ИнОУП



Ю.Г. Кирюхин

Программа одобрена методической комиссией факультета ВТ

Протокол № 2 от «15» июня 2015 года

Председатель методической комиссии факультета ВТ



Н.Н. Коннов

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Учебная группа	Решение кафедры (№ протокола, дата, подпись зав. кафедрой)	Решение выпускающей кафедры (№ протокола, дата, подпись зав. кафедрой)	Лектор	Изменение №
2017/2018	15 ВД1		Уч. без измен. протокол № от 31.01.2017 Зав. каф. ИИИ	Печерский	
2018/2019	16 ВД1		Уч. без изменений протокол № от 10.09.2018 Зав. каф. ИИИ	Печерский	
2019/2020	17 ВД1		Уч. без изменений протокол № от 20.02.19 Зав. каф. ИИИ	Печерский	