Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
**«Пермский национальный исследовательский
политехнический университет»**

Лысьвенский филиал
Кафедра естественнонаучных дисциплин

СОГЛАСОВАНО	УТВЕРЖДАЮ
Зам. директора по УР	Директор ЛФ ПНИПУ
_____ Н.Н. Третьякова	_____ В.А. Кочнев
«26» 12 2014 г.	«26» 12 2014 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

«Информационная безопасность предприятия»

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Основной образовательной программы подготовки бакалавров
Направление «38.03.01 (080100.62) Экономика»

Профиль подготовки	**Бухгалтерский учёт, анализ и аудит**
Квалификация (степень) выпускника	**бакалавр**
Специальное звание выпускника	**-**
Выпускающая кафедра	**Гуманитарных и социально-экономических дисциплин**
Форма обучения	**очная**

Курс: 3 **Семестр(ы):** 6

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕТ
Часов по рабочему учебному плану: 148 Ч

Виды контроля:
Экзамен: - Дифференцированный зачёт: 6 Курсовой проект: - Курсовая работа: -

Лысьва 2014 г.

Аннотация рабочей программы дисциплины «Информационная безопасность предприятия» разработана на основании:

- Федерального государственного образовательного стандарта высшего профессионального образования, утверждённого приказом Министерства образования и науки российской Федерации «21» декабря 2009 г. номер приказа 747 по направлению подготовки 080100 Экономика;
- Компетентностной модели (КМ) выпускника ООП по направлению подготовки 080100 Экономика, утверждённой «24» июня 2013 г.;
- Базового учебного плана очной формы обучения по направлению 080100 Экономика, по профилю подготовки Бухгалтерский учёт, анализ и аудит, утверждённого «29» августа 2011 г.

Аннотация рабочей программы согласована с рабочими программами дисциплин «Правоведение», «Информатика», «Информационно-правовые системы», «Информационные системы управления», «Компьютерные системы бухгалтерского учёта 1С», участвующих в формировании компетенций совместно с данной дисциплиной.

Разработчик ст. преподаватель _____ Кочнев П.В.

Аннотация рабочей программы рассмотрена и одобрена на заседании кафедры Естественнонаучных дисциплин «10» декабря 2014 г., протокол № 14.

Заведующий кафедрой,
ведущей дисциплину _____ Хаматнурова Е.Н.

Согласовано

Начальник учебно-методического
отдела _____ Рыданных О.В.

Специалист УМО по кафедре ЕН _____ Щукина А.А.

1. Общая информация о дисциплине

1.1. Название дисциплины: **Информационная безопасность предприятия**

1.2. Трудоёмкость дисциплины

1.2.1. Трудоёмкость дисциплины по учебному плану очной формы обучения:

148 часов (4 ЗЕ) из них:
лекций – 16 час.
лабораторных занятий – 0 час.
практических занятий – 36 час.
самостоятельной работы студентов – 94 час.
контроль самостоятельной работы – 2 час.

1.2.2. Трудоёмкость дисциплины по учебному плану заочной формы обучения, реализуемой в сокращённые сроки:

148 часов (4 ЗЕ) из них:
лекций – 4 час.
лабораторных занятий – 0 час.
практических занятий – 6 час.
самостоятельной работы студентов – 132 час.
контроль самостоятельной работы – 2 час.
итоговый контроль – 4 час.

1.3. Место дисциплины в рабочем учебном плане 080100.62 Экономика: дисциплина вариативной части математического и естественнонаучного цикла дисциплин. Обязательные предшествующие дисциплины – Информатика, Информационные технологии в экономике.

2. Цель и задачи предметного обучения

2.1. Цель изучения дисциплины – формирование знаний о методах и средствах защиты информации на предприятии.

2.2. Задачи изучения дисциплины:

- изучение действующей нормативной документации по вопросам компьютерной безопасности, формальной модели безопасности, технологии построения защищенных компьютерных систем;
- формирование умений и навыков применять средства защиты информации на предприятии.

2.3. Предметом изучения дисциплины являются следующие объекты:

- источники атак на информацию;
- модели и политики информационной безопасности предприятия;
- нормативные документы по защите информации на предприятии.

3. Результаты предметного обучения

3.1. Дисциплина участвует в формировании следующей компетенции:

Общекультурной:

- способен 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-12).

3.2. Освоение дисциплины предполагает достижение следующих результатов обучения (компонентов перечисленных выше компетенций):

Знать:

- источники атак на информацию и риски, к которым приводят атаки на информацию;
- основные атаки изнутри и снаружи системы;
- механизмы защиты от атак;
- принципы действия и основные разновидности антивирусного программного обеспечения;
- основные этапы разработки концепции и создания системы информационной безопасности в автоматизированной системе (АС) предприятия;
- основные методы правовой защиты информации в АС;
- основные методы защиты конфиденциальной информации при использовании государственных систем лицензирования и сертификации.

Уметь:

- реализовать простейший генератор паролей, обладающий требуемой стойкостью к взлому;
- использовать методы лицензирования и сертификации для работы предприятия.

Владеть:

- основными приёмами анализа защищённости предприятия;
- основными приёмами выбора средств защиты предприятия;
- основными приёмами противостояния угрозам нарушения конфиденциальности, целостности и доступности информации на предприятии.

4. Структура и модульное содержание дисциплины Информационная безопасность предприятия

4.1. Очная форма обучения

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов							Трудоём-кость всего	
			Аудиторная работа				КСР	СР	Аттестация		
			всего	Л	ПЗ	ЛР				час.	з.е.
Мод 1	Раздел 1. Источники атак на информацию	Тема 1. Введение	1	1				6		7	
		Тема 2. Основные понятия и определения компьютерной безопасности	1	1				6		7	
		Тема 3. Общие проблемы безопасности	1	1				6		7	
		Тема 4. Требования к системам защиты информации	1	1			0,5	6		7	
		Итого по модулю:	***4***	***4***			***0,5***	***24***		***28,5***	***0,79***
Мод 2	Раздел 2. Модели и политики безопасности	Тема 5. Международные стандарты компьютерной безопасности	1	1				4		5	
		Тема 6. Нормативные документы в сфере компьютерной безопасности на уровне государства	1	1				4		5	
		Тема 7. Возможные нарушения компьютерных систем и защита от возможных нарушений	6	2	4			4		10	
		Тема 8. Формальные модели безопасности и их применение	3	1	2			4		7	
		Тема 9. Нарушения компьютерной безопасности на предприятии	3	1	2			4		7	
		Тема 10. Идентификация и аутентификация	1	1			0,5	4		5,5	
		Итого по модулю:	***15***	***7***	***8***		***0,5***	***24***		***39,5***	***1,1***
Мод 3	Раздел 3. Информационная безопасность предприятия	Тема 11. Служебная тайна	7	1	6			8		15	
		Тема 12. Конкурентная разведка и промышленный шпионаж	7	1	6		0,5	8		15,5	
		Тема 13. Проведение анализа риска	7	1	6			8		15	

	Итого по модулю:		***21***	***3***	***18***		***0,5***	***24***		***45,5***	***1,26***
Мод 4	Раздел 4. Лицензирование деятельности и сертификация средств в области защиты конфиденциальной информации	Тема 14. Освоение методов защиты конфиденциальной информации при применении государственных систем лицензирования и сертификации	6	1	5			10		16	
		Тема 15. Реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому	6	1	5		0,5	12		18,5	
	Итого по модулю:		***12***	***2***	***10***		***0,5***	***22***		***34,5***	***0,96***
Итоговая аттестация:									**дифф. зачёт**		
Итого за семестр:			**52**	**16**	**36**		**2**	**94**		**148**	**4**

4.2. Заочная форма обучения, реализуемая в сокращённые сроки

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов							Трудоём-кость всего	
			Аудиторная работа				КСР	СР	Аттестация		
			всего	Л	ПЗ	ЛР				час.	з.е.
Мод 1	Раздел 1. Источники атак на информацию	Тема 1. Введение	1	1				8		9	
		Тема 2. Основные понятия и определения компьютерной безопасности						8		8	
		Тема 3. Общие проблемы безопасности						8		8	
		Тема 4. Требования к системам защиты информации					0,5	9		9,5	
		Итого по модулю:	***1***	***1***			***0,5***	***33***		***34,5***	***0,96***
Мод 2	Раздел 2. Модели и политики безопасности	Тема 5. Международные стандарты компьютерной безопасности						5		5	
		Тема 6. Нормативные документы в сфере компьютерной безопасности на уровне государства						5		5	
		Тема 7. Возможные нарушения компьютерных систем и защита от возможных нарушений	2	1	1			5		7	
		Тема 8. Формальные модели безопасности и их применение						5		5	
		Тема 9. Нарушения компьютерной безопасности на предприятии						6		6	
		Тема 10. Идентификация и аутентификация					0,5	7		7,5	
		Итого по модулю:	***2***	***1***	***1***		***0,5***	***33***		***35,5***	***0,99***
Мод 3	Раздел 3. Информационная безопасность предприятия	Тема 11. Служебная тайна	2	1	1			11		13	
		Тема 12. Конкурентная разведка и промышленный шпионаж	1		1			11		12	
		Тема 13. Проведение анализа риска	1		1		0,5	11		12,5	

	Итого по модулю:		***4***	***1***	***3***		***0,5***	***33***		***37,5***	***1,04***
Мод 4	Раздел 4. Лицензирование деятельности и сертификация средств в области защиты конфиденциальной информации	Тема 14. Освоение методов защиты конфиденциальной информации при применении государственных систем лицензирования и сертификации	2	1	1			16		18	
		Тема 15. Реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому	1		1		0,5	17		18,5	
	Итого по модулю:		***3***	***1***	***2***		***0,5***	***33***		***36,5***	***1,01***
Итоговая аттестация:									**дифф. зачёт**	**4**	**0,11**
Итого за семестр:			**12**	**4**	**6**		**2**	**132**		**148**	**4**

4.3. Перечень тем практических занятий

№ п.п.	Номер темы дисциплины	Наименование темы практического занятия
1.	7,8,9	Применение криптографических методов защиты информации
2.	11	Закрепление права предприятия на защиту информации в нормативных документах
3.	12	Создание системы информационной безопасности предприятия
4.	13	Правовые нормы защиты информации в автоматизированных системах
5.	14	Лицензирование деятельности и сертификация средств в области защиты конфиденциальной информации
6.	15	Количественная оценка стойкости парольной защиты

5. Формы контроля

5.1. Текущий контроль освоения заданных дисциплинарных компетенций

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

- опрос, проверочная работа для анализа усвоения материала предыдущей лекции, тестирование;
- оценка работы студента на лекционных и практических занятиях в рамках рейтинговой системы.

5.2. Рубежный и промежуточный контроль освоения заданных дисциплинарных компетенций

Рубежный контроль освоения дисциплинарных компетенций проводится по окончании модулей дисциплины в следующих формах:

- контрольная работа (для студентов заочной формы обучения);
- выполнение заданий на практических занятиях (модули 2-4);
- тестирование (модули 1-4).

5.3. Итоговый контроль освоения заданных дисциплинарных компетенций

а) **Дифференцированный зачёт**

Порядок проведения дифференцированного зачёта по дисциплине

Дифференцированный зачёт по дисциплине получают студенты, имеющие положительные оценки по всем промежуточным аттестациям и выполнившие полностью все виды работ, предусмотренные в данном семестре (выполнение заданий на практических занятиях). Студенты, имеющие неудовлетворительные оценки по промежуточным аттестациям или не сдавшие один из видов работ, должны ликвидировать указанные задолженности прежде, чем они будут допущены к процедуре приёма дифференцированного зачёта.

Процедура дифференцированного зачёта по дисциплине проводится в форме собеседования со студентом по разделам дисциплины.

Результат сдачи дифференцированного зачёта оценивается следующим образом: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Все оценки, кроме «неудовлетворительно» заносятся в экзаменационную ведомость и

зачётную книжку студента, запись «неудовлетворительно» выставляется только в экзаменационную ведомость.

б) **Экзамен** не предусмотрен.

Контрольно-измерительные материалы

Перечень вопросов для подготовки к дифференцированному зачёту

1. Нормативно-правовое регулирование профессиональной тайны в РФ
2. Признаки и объекты профессиональной тайны
3. Сведения, относящиеся к служебной тайне
4. Правовые акты, на которых основана защита служебной и коммерческой информации на предприятии
5. Отличия служебной тайны от профессиональной
6. Внутренние нормативные документы, использующиеся для правовой защиты служебной и коммерческой тайны (КТ)
7. Виды договоров, входящих в условия о неразглашении служебной тайны
8. Убытки в результате разглашения КТ
9. Определение и виды конкурентной разведки
10. Этапы создания системы информационной безопасности предприятия (ИБП)
11. Реализация на практике концепции ИБП
12. Документы, на основе которых разрабатывается политика безопасности
13. Стратегические принципы безопасности
14. Уровни политики безопасности и ответственные за них
15. Анализ риска. Методы оценки рисков
16. Категории защищаемых активов АС, классификация угроз
17. План защиты АС
18. План обеспечения непрерывной работы и восстановления АС
19. Особенности расследования компьютерных преступлений
20. Задачи, решаемые судебно-бухгалтерскими и программно-техническими экспертизами при проведении следственных действий
21. Классификация компьютерных преступлений. Методы НСД
22. Методы и приемы предупреждения компьютерных преступлений. Анализ компьютерных преступлений
23. Документы, в которых представлены нормы правового обеспечения защиты информации в АС
24. Документ «Политика безопасности»
25. Документы, необходимые для представления при присвоении класса защищенности АС
26. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ
27. Правила безопасности необходимые для реализации «Политики безопасности»
28. Требования к безопасности компьютерных сетей в РФ
29. Нормативно-правовое регулирование деятельности в области защиты конфиденциальной информации

30. Виды деятельности в области защиты конфиденциальной информации
31. Порядок лицензирования, срок действия лицензии
32. Организационная структура системы сертификации в области защиты конфиденциальной информации
33. Организации, при которых созданы системы сертификации в РФ
34. Порядок и требования при осуществлении сертификации средств защиты информации
35. Условия, при которых сертификация носит добровольный характер
36. Формы сертификата и знак соответствия
37. Российские и международные стандарты безопасности
38. Стойкость подсистемы идентификации и аутентификации
39. Минимальные требования к выбору пароля
40. Вероятность подбора пароля злоумышленником в течении срока его действия
41. Параметры, которые влияют на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля

КАРТА ОБЕСПЕЧЕННОСТИ
УЧЕБНО-МЕТОДИЧЕСКОЙ ЛИТЕРАТУРОЙ
дисциплины ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Кафедра Естественнонаучных дисциплин.
Факультет высшего образования.

Направление	Семестры	Кол-во студентов	Библиографическое описание издания (автор, заглавие, вид, место, изд-во, год издания, кол-во страниц)	Кол-во экз. в библ.	Основной лектор
080100.62	4, 5, 6	63 чел.	**Основная литература** 1. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений / В.П. Мельников, С.А. Клейменов, А.М. Патраков; под ред. С.А. Клейменова. - М.: Академия, 2006. - 332 с. 2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для вузов / П.Б. Хорев. - М.: ИЦ Академия, 2005, 2006. - 256 с. **Дополнительная литература** 1. Ахметова С.Г. Информационная безопасность [электронный ресурс]. - Издательство ПНИПУ, 2013. - Режим доступа: http://lib.pstu.ru/elib 2. Галатенко В.А. Основы информационной безопасности. Курс лекций: учеб. пособие / В.А. Галатенко; под ред. В.Б. Бетелина. - 2-е изд., испр. - М.: ИНТУИТ.РУ "Интернет-Ун-т Инф. Технологий, 2004. - 264 с. 3. Комплексная система защиты информации на предприятии [электронный ресурс] / А.В. Полшков, А.С. Шабуров. - Издательство ПНИПУ, 2013. - Режим доступа: http://lib.pstu.ru/elib 4. Основы информационной безопасности [электронный ресурс] / А.Н. Данилов, С.А. Данилова, А.А. Зорин. - Издательство ПНИПУ, 2008. - Режим доступа: http://lib.pstu.ru/elib 5. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие для СПО / В.Ф. Шаньгин. - М.: ФОРУМ, 2010. - 416 с.	10 23 ЭР 23 ЭР ЭР 5	Кочнев Павел Викторович

СОГЛАСОВАНО:
Зав. отделом научной библиотеки _____ Е.А. Винокурова

Книгообеспеченность дисциплины составляет:
- основной учебной литературой: на 01.09.2014 – 0,5 экз/обуч.
(число, месяц, год) (экз. на 1 обучаемого)

- дополнительной учебной литературой: на 01.09.2014 – более 1экз/обуч.
(число, месяц, год) (экз. на 1 обучаемого)