МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Рабочая программа дисциплины

Основы управления информационной безопасностью

Кафедра **Информатики и информационных технологий**

факультета **Информатики и информационных технллогий**

Образовательная программа **09.03.02 «Информационные системы и технологии»**

Профиль подготовки

Информационные системы и технологии

Уровень высшего образования

Бакалавриат

Форма обучения

очная

Статус дисциплины: **вариативная (по выбору)**

Махачкала 2016

Рабочая программа дисциплины составлена в _2015__ году в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 «Информационные системы и технологии», профиль подготовки «Информационные системы и технологии» (уровень бакалавриат), утвержденного приказом Минобрнауки РФ от 12 марта 2015 г. № 219_, вступил в силу 30 марта 2015 г.

Разработчик: кафедра информатики и информационных технологий,
Абдуллаев Габид Шаванович, кандидат экономических наук, доцент

Рабочая программа дисциплины одобрена:
на заседании кафедры Информатики и информационных технологий
от «_5_» __07__2015г., протокол № _1_

Зав. кафедрой _____ проф. Ахмедов С.А.
(подпись) на заседании Методической комиссии факультета Информатики и информационных технологий от «__10_» ___07_____20_15_г., протокол №_6_.

Председатель _____ доц. Камилов К.Б.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «_31___» ___августа__20_15_г.

Цели дисциплины

Целями изучения дисциплины «Управление информационной безопасностью» является:

формирование навыков организации и методологии обеспечения информационной безопасности в коммерческих организациях и организациях банковской системы РФ;

создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в коммерческих организациях и организациях банковской системы РФ;

развитие способностей по использованию существующей системы управления информационной безопасности.

Место дисциплины в структуре ООП

Учебная программа дисциплины «Управление информационной безопасностью» является дисциплиной базовой части профессионального цикла дисциплин ООП по направлению 090900.62 «Информационная безопасность» (бакалавриат).

Изучение дисциплины базируется на знаниях, полученных студентами при изучении дисциплин «Надежность информационных систем», «Администрирование в информационных системах», «Информационная безопасность и защита информации», «Технологии обработки информации». Изучение дисциплины позволяет овладеть как теоретической базой, так и конкретными практическими навыками по организации и управлению информационной безопасностью.

Требования к результатам освоения дисциплины

В совокупности с дисциплинами базовой и вариативной части профессионального цикла ФГОС ВПО дисциплина «Управление информационной безопасностью» обеспечивает инструментарий формирования следующих общекультурных (ОК) и профессиональных (ПК) компетенций:

№ п/п	Код	Компетенция	Формы и методы обучения
1	ПК-8	Способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	Лекции. Практические занятия. Работа с источниками и поиск информаций в Интернете. Решение проблемных задач связанных с методологией управления информационной безопасностью.
2	ПК-9	Умение использовать современные стандарты и методики, разрабатывать регламенты для организации и управления процессами жизненного цикла ИТ-инфраструктуры предприятий	

3	ПК–14	Способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности	Обсуждение актуальных вопросов, связанных с перспективными направлениями развития науки и техники в области защиты информации. Выступления студентов с докладами и презентациями.
4	ПК-21	Способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.	
5	ПК–29	Способность участвовать в работах по реализации политики информационной безопасности.	
6	ПК–30	Способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности.	

 В результате освоения дисциплины «Управление информационной безопасностью» студент должен:

знать:

 основные понятия, термины, определения в бизнес-процессах, а также понятия анализа видов информации, в которых данные процессы проявляются: учредительная и лицензионная база организации, правовая сфера бизнеса, внутренняя нормативная база организации, внешняя и внутренняя отчетность, материальные и информационные активы;

 основные методики оценки уровня информационной безопасности организации и примеры их использования;

 основные методы противодействия «внутренним» угрозам информационной безопасности организации;

 архитектуру основных стандартов защиты информации;

уметь:

 использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации, методы противодействия «внутренним» угрозам информационной безопасности организации, методы анализа рисков информационной безопасности, методы организационного проектирования, методы управления информационными активами организации;

Владеть навыками:

 использования методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации как систематической практической деятельности коллегиальных органов управления организацией и руководителя службы, направленной на формирование и поддержание концептуальных и организационных основ деятельности организации и эффективное выполнение поставленных задач.

Объём дисциплины и виды учебной работы

Общая трудоемкость дисциплины «Управление информационной безопасностью» составляет 3 зачётные единицы.

Вид промежуточной аттестации – зачет.

Вид учебной работы	**Часы**	**Семестр**
		7
Общая трудоёмкость дисциплины	**108**	**108**
Аудиторные занятия	**50**	**50**
Лекции (Л)	16	16
Практические и семинарские занятия (ПЗ)	16	16
Лабораторные занятия	18	18
Самостоятельная работа (СР)	**58**	**58**

Содержание дисциплины

Часть 1. Содержание дисциплины

Раздел 1. Основы построения систем обеспечения информационной безопасности на предприятии

Деятельность по обеспечению информационной безопасности. Предметная направленность деятельности по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности. Принципы и форма деятельности по обеспечению информационной безопасности. Методы деятельности по обеспечению информационной безопасности. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.

Раздел 2. Обеспечение информационной безопасности бизнеса Информационная сущность бизнеса. Роль руководства организации в обеспечении информационной безопасности. Определение информационной безопасности. Правовая среда бизнеса и ее свойства. Внутренняя нормативная база организации. Модель информационной безопасности бизнеса. Обобщенная модель распределения ресурсов организации в условиях рисков. Ущерб и негативные последствия. Риск- ориентированный подход к обеспечению информационной безопасности бизнеса. Общая модель обеспечения ИБ бизнеса.

Раздел 3. Система управления информационной безопасностью бизнеса

Модели непрерывного совершенствования и корпоративное управление. Модели непрерывного совершенствования и международные стандарты. Шаги реализации стандартной системы управления информационной безопасностью организации. Модели COSO, COBIT, ITIL. Контроль и аудит.

Раздел 4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса

Способы оценки информационной безопасности. Основные элементы

процесса оценки информационной безопасности. Способы измерения атрибутов объекта оценки информационной безопасности. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности.
Модель оценки информационной безопасности на основе оценки процессов. Риск-ориентированная оценка информационной безопасности.

Раздел 5. Управление жизненным циклом информационных активов. Анализ влияния состояния информационных активов на деятельность организации

Жизненный цикл искусственно созданных объектов. Теротехнология. Информационный актив. Распределение информационных систем по целевым направлениям. Совместное использование данных в организации. Формирование стоимости владения информационным активом. Модель BSI PAS 99. Ценность и стоимость информационного актива. Уровни критичности информационного актива. Понятие «Анализ воздействия на бизнес». Структура управления операционным риском организации.

Раздел 6. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.

Рискообразующие факторы. Структура информационного риска. Понятие «Риск информационной безопасности». Методика анализа риска информационной безопасности. Обработка рисков информационной безопасности. Процесс «Управление рисками информационной безопасности». Место управления рисками информационной безопасности в структуре управления операционными рисками организации. Место управления рисками информационной безопасности в структуре управления информационной безопасностью организации.

Раздел 7. Подходы к формированию нормативного обеспечения системы информационной безопасности организации

Анализ нормативной базы организации. Делопроизводство и документооборот организации. Процесс управления документацией. Защищённый документооборот. Информационный обмен. Жизненный цикл документа. Структура документации системы управления информационной безопасностью. Понятие «запись». Процесс уничтожения документации.

Раздел 8. Аудит методов и средств обеспечения информационной безопасности организации

Аудит информационной безопасности. Стандарты и практики аудита информационной безопасности. Международный стандарт ISO 19011. Методы организации, подготовки и проведения аудита информационной безопасности. Обработка результатов аудита. Понятие
«Корректирующие» и «Превентивные» мероприятия. Аудит интегрированных систем управления. Психологические аспекты подготовки аудитора информационной безопасности. Понятие «независимая оценка» состояния информационной безопасности организации. Ответственность за результаты аудиторской проверки. Место аудита информационной безопасности в структуре управления информационной безопасностью организации.

Часть 3. Темы дисциплины и виды учебных занятий (учебно – тематический план)

№ п/ п	Наименование темы дисциплины	Трудоёмкость в часах					
		Всего часов		Аудиторная работа			СР
			Общая	лек		ПЗ	
1.	Основы построения систем обеспечения информационной безопасности на предприятии.	5	6	2	2	2	4
2.	Обеспечение информационной безопасности бизнеса.	5	6	2	2	2	4
3.	Система управления информационной безопасностью бизнеса.	10	6	2	2	2	8
4.	Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.	6	6	2	2	2	8
5.	Управление жизненным циклом информационных активов. Анализ влияния состояния информационных активов на деятельность организации.	8	6	2	2	2	8
6.	Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.	10	6	2	2	2	8
7.	Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.	6	6	2	2	2	8
8.	Аудит методов и средств обеспечения информационной безопасности организации.	6	8	2	2	4	10
	Итого по семестру	***108***	***50***	***16***	***16***	18	***58***

Практические и семинарские занятия

№ п/п	№ темы дисцип-лины	Тематика практических занятий (семинаров)	Технология проведения	Трудоём-кость в часах
1	**1-4**	Анализ и оценка управленческих и экономических показателей системы управления обеспечением информационной безопасности бизнеса.	Теоретическая справка с кратким изложением основных понятий. Проведение ситуационных моделей происходит в интерактивной форме для отработки навыков управления	6
2	**5-6**	Управление жизненным циклом информационных активов.		4

3	**7-8**	Анализ влияния информационного риска на деятельность организации.	информационной безопасностью Выступления студентов с докладами и презентациями. Аудиторные самостоятельные работы для качественной оценки пройденного материала (15-20 мин.).	6
		ИТОГО		16

Самостоятельная работа

При изучении дисциплины «Управление информационной безопасностью» обязательными являются следующие виды самостоятельной работы:

- разбор теоретического материала по учебным пособиям и конспектам лекций;
- самостоятельное изучение указанных теоретических вопросов; подготовка к проведению ситуационных моделей в интерактивной форме;

№ темы дисциплины	Форма самостоятельной работы	Трудоемкость в часах
1–8	Работа с учебной литературой. Разбор вопросов по теме занятия. Работа с источниками и поиск информаций в Интернете. Подготовка устного доклада. Подготовка к самостоятельной проверочной работе.	32
1-8	Выполнение контрольной работы.	16
4, 6	Подготовка к интерактивному занятию	10
Итого:		**58**

Система оценивания

Уровень требований и критерии оценок

Текущий контроль усвоения знаний по дисциплине «Управление информационной безопасностью» осуществляется в течение семестра в ходе учебного процесса и консультирования студентов, по результатам выполнения аудиторных самостоятельных проверочных работ, контрольной работы и активного участия в проведении занятия в интерактивной форме.

- Основными формами текущего контроля знаний являются: решение проблемных задач по управлению информационной безопасностью;
- участие в обсуждении актуальных вопросов, связанных с введением новых требований по обеспечению информационной безопасности предприятий различных форм собственности, в проведении занятия в интерактивной форме;

- собеседование по теоретическим вопросам;
- выполнение аудиторных самостоятельных работ, контрольной работы, обсуждение и анализ их результатов. Промежуточная аттестация (экзамен) проводится в письменной форме в виде ответов на вопросы билета. Оценка знаний студентов осуществляется в баллах с учетом: оценки за работу в семестре (за: по управлению информационной безопасностью, успешное выполнение контрольной и самостоятельных проверочных работы, активное участие в обсуждениях на практических занятиях и др.); оценки итоговых знаний в ходе экзамена.

Оценка знаний студентов осуществляется по 100-балльной шкале в соответствии с критериями Финансового университета и реализуются следующим образом:

Требования к результатам освоения дисциплины	**Оценка или зачет**	**Баллы** (рейтиговая оценка)
Глубокое усвоение программного материала, связанного со знанием понятийного аппарата, определением в бизнес-процессах, методик оценки уровня информационной безопасности организации и примеров их использования, методов противодействия «внутренним» угрозам информационной безопасности организации, архитектуры основных стандартов защиты информации; умением использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации, методы противодействия «внутренним» угрозам информационной безопасности организации, методы анализа рисков информационной безопасности, методы организационного проектирования, методы управления информационными активами организации; владением навыками использования методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации, а также логически стройное его изложение, умение применить теоретические знания для решения задач, свободное решение задач и обоснование принятого решения, выполнение текущей работы в семестре.	*отлично*	*86-100*

Твердые знания программного материала, связанного понятийным аппаратом, бизнес- процессов, методик оценки уровня информационной безопасности организации и примеров их использования, методов противодействия «внутренним» угрозам информационной безопасности организации, архитектуры основных стандартов защиты информации; умением использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации, методы противодействия «внутренним» угрозам информационной безопасности организации, методы анализа рисков информационной безопасности, методы организационного проектирования, методы управления информационными активами организации; владением навыками использования методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации, а также грамотное и по существу его изложение, допустимы несущественные неточности в ответе на вопрос, правильное применение теоретических положений при решении практических вопросов и задач, выполнение текущей работы в семестре.	*хорошо*	*66-85*
Знание только основного материала, понятийного аппарата, определением в бизнес-процессах, методик оценки уровня информационной безопасности организации и примеров их использования; умением использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации, методы противодействия «внутренним» угрозам информационной безопасности организации,	*удовлетв.*	*51-65*
методы анализа рисков информационной безопасности, методы организационного проектирования; владением навыками использования методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации, а также допустимы неточности в ответе на вопрос, недостаточно правильные формулировки, нарушение логической последовательности в изложении теоретического материала, затруднения при решении практических задач, выполнение текущей работы в семестре.		
Незнание значительной части программного материала, неумение сформулировать правильные ответы на вопросы экзаменационного билета, невыполнение практических заданий.	неудовлетв.	0-50

Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература
а) основная:

1. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.Международный стандарт. ISO/IEC 27000:2005 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы./ http://www.27000.org/
2. Аудит информационной безопасности. Под ред. А.П.Курило. – М: БДЦ-Пресс, 2014.
3. Галатенко В.А. Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий, 2006 г. – 264 с.
4. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005)./ http://www.27000.org/
5. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью./ http://www.27000.org/Международный стандарт. ISO/IEC 27003:2005 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью./ http://www.27000.org/
6. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью./ http://www.27000.org/
7. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности./ http://www.27000.org/
8. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью./ http://www.27000.org/
9. Международный стандарт. ISO/IEC 27007:2005 Информационные технологии. Методы обеспечения безопасности. Руководство для аудитора систем управления информационной безопасностью./ http://www.27000.org/
10. Минаев В.А., Фисун А.П. Правовое обеспечение информационной безопасности, Москва, 2014.
11. Петренко С., Симонов С. Управление информационными рисками. Экономически оправданная безопасность. — М.: АйТи-Пресс, 2012.
12. Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: ДМК пресс, 2013.
13. Репин В., Елиферов В. Процессный подход к управлению. Моделирование бизнес-процессов. М.: Стандарты и качество, 2014.
14. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. – М.: Академия, 2008 г. – 192 стр.
15. Тихонов В., Райх В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. – М.: Гелиос АРВ, 2012.

б) дополнительная:

1. Золотарев Управление информационной безопасностью. Ч. 1. Анализ информационных рисков - Красноярск: Сибирский государственный

аэрокосмический университет имени академика М. Ф. Решетнева, 2010.

Материально-техническое обеспечение дисциплины

В качестве материально-технического обеспечения дисциплины «Управление информационной безопасностью» используются мультимедийные средства, компьютерные симуляторы, графические презентационные материалы.