МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СЕРВИСА»
(ФГБОУ ВО «ПВГУС»)

Кафедра Прикладная информатика в экономике

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

по дисциплине «Основы управления информационной безопасностью»
для студентов направления подготовки 10.03.01 «Информационная безопасность»
направленности (профиля) «Организация и технология защиты информации»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине «Основы управления информационной безопасностью» включена в основную профессиональную образовательную программу направления подготовки 10.03.01 «Информационная безопасность» направленности (профиля) «Организация и технология защиты информации» решением Президиума Ученого совета

Протокол № 4 от 28.06.2018 г.

Начальник учебно-методического отдела_____ Н.М.Шемендюк

28.06.2018 г.

Рабочая учебная программа по дисциплине «Основы управления информационной безопасностью» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Минобрнауки РФ от 01.12.2016 г. № 1515

Составил: д.э.н.. Бердников В. А.

Согласовано Директор научной библиотеки_____ В.Н.Еремина

Согласовано Начальник управления информатизации_____В.В.Обухов

Рабочая программа утверждена на заседании кафедры
«Прикладная информатика в информационной сфере»
Протокол № 12 от «22» июня 2018г.

И.о. заведующего кафедрой _____д.э.н., Бердников В.А._____

Согласовано начальник учебно-методического отдела _____ Н.М.Шемендюк

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Цели освоения дисциплины

Целью освоения дисциплины являются:

- получение необходимых знаний о принципах и методах, инструментальных средств, нормативных документах регуляторах, позволяющих успешно управлять информационной безопасность организации в условиях активного использования информационных технологий.

1.2. В соответствии с видами профессиональной деятельности - организационно-управленческая, научно-исследовательская - аналитическая, на которые ориентирована образовательная программа направления подготовки 10.03.01 «Информационная безопасность», содержание дисциплины позволит обучающимся решать следующие профессиональные задачи:

- проведение обследования прикладной области в соответствии с профилем подготовки;
- применение системного подхода к информатизации и автоматизации решения прикладных задач;
- построению информационных систем на основе современных информационно-коммуникационных технологий и математических методов;
- участие в организации информационно-телекоммуникационной инфраструктуры;
- управлении основами информационной безопасностью информационных систем;
- применение системного подхода к информатизации и автоматизации решения прикладных задач.

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины у обучающихся формируются следующие компетенции:

Код компетенции	Наименование компетенции
ОПК-5	Способность использовать нормативные правовые акты в профессиональной деятельности.
ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

1.4. Перечень планируемых результатов обучения по дисциплине «Основы управления информационной безопасностью» направление подготовки 10.03.01 «Информационная безопасность»

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
Знает: ***ОПК-5*** нормативные акты и стандарты в области управления информационной безопасностью ***ОПК-7*** принципы построения информационных систем; принципы организации информационных систем в соответствии с требованиями по защите информации	Лекции, практические занятия.	Собеседование, подготовка рефератов, докладов
Умеет: ***ОПК-5***	Лекции, практические занятия,	собеседование, подготовка рефератов, докла-

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
выполнять планирование, идентификацию и анализ рисков, моделировать риски, проводить мониторинг. ***ОПК-7*** анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах.	индивидуальные задания, использование интернет ресурсов.	дов
Имеет практический опыт: ***ОПК-5*** управления информационной безопасность предприятия в условиях применения современных информационных технологий. ***ОПК-7*** анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации; принятие мер защиты информации при выявлении новых угроз безопасности информации; уточнения модели угроз безопасности информации автоматизированной системы.	Лекции, практические занятия, самостоятельная работа, использование интернет ресурсов.	собеседование, защита индивидуальных заданий, подготовка рефератов, докладов

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части направления подготовки 10.03.01 «Информационная безопасность». Ее освоение осуществляется в 7 семестре у студентов дневной формы обучения и в 8 семестре у студентов очно-заочной форме обучения.

№ п/п	Наименование дисциплин, определяющих	Код и наименование компетенций

	междисциплинарные связи	
	Предшествующие дисциплины (практики)	
	Компьютерный практикум	ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.
	Последующие дисциплины (практики)	
	Защита информационных процессов в компьютерных системах и телекоммуникационных сетях	ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.
	Информационно-аналитическая деятельность по обеспечению комплексной безопасности	ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации. ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Распределение фонда времени по семестрам и видам занятий
направление подготовки 10.03.01 «Информационная безопасность»

Виды занятий	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Итого часов Зачетных единиц	108 ч. 3 з.е.	108 3 з.е	_
Лекции (час)	18	4	
Практические (семинарские) занятия (час)	28	8	-
Лабораторные работы (час)	-	-	-
Самостоятельная работа (час)	62	92	-
Курсовой проект (работа) (+,-)	-	-	-
Контрольная работа (+,-)	-	-	-
Экзамен, семестр /час.	-	8 / 4	-
Зачет, семестр / час.	-	-	-
Контрольная работа, семестр	-	-	-

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины	Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в академических часах)				Средства и технологии оценки
		Лекции, час	Практические занятия, час	Лабораторные работы, час	Самостоятельная работа, час	
1	Тема 1. Концепция управления информационной безопасностью. Базовая терминология.	2/0,3/-	2/1/-	-/-/-	6/12/-	устный опрос, индивидуальное задание
2	Тема 2. Стандартизация систем и процессов управления информационной безопасностью.	4/1/-	4/1/-	-/-/-	10/16/-	устный опрос, индивидуальное задание
3	Тема 3.Политика информационной безопасности.	2/0,8/-	6/1/-	-/-/-	10/14/-	устный опрос, индивидуальное задание
4	Тема 4. Управление и система управления информационной безопасностью.	2/0,3/-	4/1/-	-/-/-	8/12/-	устный опрос, индивидуальное задание
5	Тема 5. Технические аспекты управления информационной безопасностью.	2/0,3/-	4/1/-	-/-/-	8/12/-	устный опрос, индивидуальное задание
6	Тема 6. Организационные и кадровые вопросы управления информационной безопасностью.	2/0,3/-	4/1/-	-/-/-	10/12/-	устный опрос, индивидуальное задание
7	Тема 7. Организационно-правовое обеспечение информационной безопасности.	4/1/-	4/1/-	-/-/-	10/14/-	устный опрос, индивидуальное задание
	Промежуточная аттестация по дисциплине	18/4/-	28/8/-	-/-/-	62/92/-	экзамен

4.2.Содержание практических (семинарских) занятий

№	Раздел дисциплины	Объем часов	Наименование темы дисциплины
	7/8 семестр		
1	Практическая работа 1. Концептуально описать процесс управления ИБ и его составляющих. Определить основные понятия, от-	8/2/-	Тема 1. Концепция управления информационной безопасностью. Базовая терминология.

	носящиеся к управлению информационной безопасностью.		
2	Практическая работа 2. Дать подробный анализ текущей ситуации в области стандартизации управления ИБ	4/2/-	Тема 2. Стандартизация систем и процессов управления информационной безопасностью.
3	Практическая работа 3. Рассмотреть основные требования и принципы, учитываемые при разработке и внедрения политики ИБ. Содержание политики ИБ. Охарактеризовать жизненный цикл политики ИБ.	6/2/-	Тема 3.Политика информационной безопасности.
4	Практическая работа 4. Исследовать систему управления ИБ организации. Рассмотреть основные процессы СУИБ. Описать стратегию построения и внедрения СУИБ.	6/2/-	Тема 4. Управление и система управления информационной безопасностью.
5	Практическая работа 5. Рассмотреть технические аспекты управления ИБ. Определить взаимосвязь системы управления ИБ с системой физзащиты объекта и мер по защите от воздействия окружающей среды.	6/2/-	Тема 5. Технические аспекты управления информационной безопасностью.
6	Практическая работа 6. Проанализировать организационные и кадровые вопросы управления ИБ. Корпоративное нормативное регулирование. Организация объектовых режимов безопасности	6/2/-	Тема 6. Организационные и кадровые вопросы управления информационной безопасностью.
7	Практическая работа 7. Рассмотреть законодательство об информации, информационных технологиях, защите информации, государственной тайне, коммерческой, персональных данных, электронной цифровой подписи, в области интеллектуальной собственности, технического регулирования.	6/2/-	Тема 7. Организационно-правовое обеспечение информационной безопасности.
	Итого за 7/8 семестр	28/8/-	
	Итого	28/8/-	

4.3.Содержание лабораторных работ

Лабораторные работы по дисциплине учебным планом не предусмотрены

5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студента является важным фактором успешного изучения дисциплины «Основы управления информационной безопасностью». Домашние, индивидуальные задания, подготовка к аудиторным занятиям, контрольным мероприятиям соответствует выделенным долям времени для среднего студента.

Эффективная система контроля обеспечивает планомерную самостоятельную работу. Сюда относятся контрольные и проверочные работы, защита научно-исследовательской работы и подготовка докладов, работа с пройденным материалом для подготовки к тестированию, опрос по теории на практических занятиях, зачет и экзамен. Текущий и рубежный контроль можно проводить в форме тестирования или в традиционной форме (письменная работа по билетам).

Самостоятельная работа студента включает в себя самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, для чего студенты должны самостоятельно изучить конспекты лекций, соответствующие разделы рекомендуемой литературы, выполнить необходимые задания. Самостоятельная работа призвана обеспечить закрепление полученных студентами знаний во время аудиторных занятий путем повторения пройденного материала.

Код реализуемой компетенции	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов
1	2	3	4	5
7 / 8 семестр				
ОПК-5, ОПК-7	Самостоятельное изучение тем: Тема 1. Концепция управления информационной безопасностью. Базовая терминология. Тема 2. Стандартизация систем и процессов управления информационной безопасностью. Тема 3.Политика информационной безопасности. Тема 4. Управление и система управления информационной безопасностью. Тема 5. Технические аспекты управления информационной безопасностью. Тема 6. Организационные и кадровые вопросы управления информационной безопасностью. Тема 7. Организационно-правовое обеспечение информационной безопасности. Выполнение научно-исследовательской работы. Подготовка к лекционным и практическим занятиям,	Конспект. Составление справочного материала. Индивидуальное задание. Доклад. Презентация НИР. Эссе. Тезирование. Статья. Опрос студентов.	Собеседование. Основная и дополнительная литература. Интернет-ресурсы. Индивидуальные задания составленные преподавателем. Конспекты аудиторных занятий.	62/92

	работам.			
Итого за 7/8 семестр: 62 ч. / 92 ч.				

При самостоятельном изучении тем используется литература, указанная в п.8.

Кроме того, студенты могут использовать интернет – ресурсы.

5.1. Содержание заданий для самостоятельной работы

Темы для выполнения заданий на самостоятельную работу

1. Серия стандартов ISO/IEC 2700 «Информационные технологии. Методы обеспечения безопасности».
2. Субъективность и ограничения традиционных и не традиционных каналов утечки информации.
3. Субъекты и объекты защиты на рынке информационных продуктов и услуг, управление их защитой.
4. Информационные ресурсы в негосударственной сфере как объекты обеспечения безопасности.
5. Отраслевые стандарты ИБ в России.
6. Управление информационными войнами и информационно-программным оружием.
7. Отраслевые стандарты в области управления ИБ – стандарты банковской системы Российской Федерации.
8. Историческое развитие понятий информации и информационных ресурсов, владение информацией как фактор формирования информационной элиты.
9. Состояние современных информационных факторов угроз личности, общества, государства и субъектам хозяйствования.
10. Методы и способы оценки вероятности наступления угроз, управление противодействием.
11. Юридическая ответственность при обеспечении информационной безопасности.
12. Возможные методы давления на пользователей как угрозы для ИБ.
13. Индикаторы и измерения для опасностей в СУИБ.
14. Криминальный характер компьютерных преступлений.
15. «Обиженные сотрудники» и исходящие от них потенциальные угрозы.
16. Психологические приемы получения закрытой информации.
17. Организационные системы обеспечения безопасности информации.
18. Разрушение СУИБ.

Тематика самостоятельных работ может быть расширена по согласованию с преподавателем.

Письменные работы могут быть представлены в следующих формах:

- статья - законченное авторское произведение, описывающее результаты исследования и/или посвящённая рассмотрению ранее опубликованных научных статей, связанных общей темой, соответствующее требованиям издателя и опубликованное.

- эссе - прозаическое сочинение небольшого объема и свободной композиции, выражающее индивидуальные впечатления и соображения по конкретному поводу или вопросу и заведомо не претендующее на определяющую или исчерпывающую трактовку предмета.

- тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала.

5.2. Вопросы для самоконтроля

5.2.1. Что понимается под информационным обществом, каковы его характерные черты?

5.2.2. Основные направления развития менеджмента в сфере управления информационной безопасности?
5.2.3. Почему информация – это стратегический ресурс?
5.2.4. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?
5.2.5. Приведите конкретные примеры охраняемых объектов (по группам).
5.2.6. Почему человек считается универсальным носителем и производителем информации?
5.2.7. Кто может являться субъектом управления ИБ?
5.2.8. Приведите примеры реальных элементов ИБ в вашем учебном заведении, относящихся к разным направлениям?
5.2.9. Каковы отличительные черты серии стандартов ISO/IEC 2700?
5.2.10. Почему построение комплекса ИБ требует системного подхода?
5.2.11. Какую информацию можно отнести к защищаемой? Приведите примеры.
5.2.12. Что можно сказать о зависимости степени секретности информации и уровня защиты, ее стоимости и круге лиц, допущенных к ней?
5.2.13. Кто в нашем государстве обеспечивает сохранность сведений, составляющих государственную или коммерческую тайны?
5.2.14. Деятельность каких служб связана с организацией и предотвращением утечек информации?
5.2.15. Каковы основные направления разведывательной деятельности иностранных спецслужб, а также конкурентов компании или предприятия в сфере промышленного шпионажа?
5.2.16. Попытайтесь сформулировать правила для предотвращения коммерческого шпионажа.
5.2.17. Приведите примеры гласных (легальных) методов получения защищаемой информации.
5.2.18. Опишите развитие возможных ситуация с закрытой информацией при ее утечке. Проиллюстрируйте примерами.
5.2.19. Чем отличаются разглашение, раскрытие или распространение? Приведите примеры.
5.2.20. Выделите условия, способствующие утечке защищаемой информации. Приведите примеры.
5.2.21. Что понимается под абстрактной угрозой?
5.2.22. Что характеризует угрозы с точки зрения ИБ?
5.2.23. Чем отличаются злоумышленники от нарушителей? Приведите примеры.
5.2.24. Какие могут быть уязвимые места в ИБ? Приведите примеры.
5.2.25. Что понимается под «заплатами», устанавливающимися в защищаемую ИБ?
5.2.26. Приведите примеры случайных или непреднамеренных угроз и продумайте способы и средства защиты.
5.2.27. Приведите примеры преднамеренных угроз и продумайте способы защиты.
5.2.28. Наступление каких угроз можно предсказать с определенной вероятностью?
5.2.29. Что относится к активам предприятия или организации? Как реализация атаки на активы скажется на ее дальнейшей работе?
5.2.30. Перечислите, реализация каких атак повлияет на бизнес и снизит ИБ.
5.2.31. Почему важно применять один подход ко всем активам при решении вопросов реализации ИБ?
5.2.32. Почему важно продумать план возврата при анализе наступления угроз ИБ?
5.2.33. Дайте характеристики различным методам дублирования информации в ИБ.

Рекомендуемая литература:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18

5.3. Примерная тематика вопросов для экзамена

1. Как определяются понятие системы и каковы основные свойства системы.
2. Роль процессов в терминах системного подхода к организации, кто может и должен определить цели бизнес-процессов.
3. Отличия понятий «менеджмент» и «управление», основные функции управления.
4. Основные направления развития менеджмента в сфере управления информационной безопасности
5. Примеры современных технологий защиты информации, основанных на различных базовых сервисах, для механизмов и инструментов защиты информации:
6. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности.
7. Международные организации в сфере информационной безопасности.
8. Международные стандарты серии 2700.
9. ISO/IEC 27000:2009 – СУИБ: определения и основные принципы.
10. Глобальные ИТ-компании в сфере информационной безопасности.
11. Основные направления, задачи и функции управления информационной безопасностью на уровне крупных поставщиков информационных систем.
12. Основные направления внешней организационной работы компании в сфере информационной безопасности.
13. Основные направления внутренней организационной работы компании в сфере информационной безопасности.
14. Содержание, основные направления управления информационной безопасностью на государственном уровне.
15. «О безопасности критической информационной инфраструктуры Российской Федерации от 26.07.2017 № 187-ФЗ»
16. Структура государственных органов, реализующих функции управления информационной безопасностью на государственном уровне.
17. «ГосСопка в рамках реализации Федерального закона О безопасности критической информационной инфраструктуры Российской Федерации от 26.07.2017 № 187-ФЗ»
18. Функции управления информационной безопасностью.
19. Разработка государственных стандартов, относящихся к организации и технологиям защиты.
20. Осуществление международного сотрудничества в сфере защиты информации
21. Основные направления менеджмента информационной безопасности на уровне предприятия.
22. Структура политики информационной безопасности.
23. Структура первого уровня политики информационной безопасности.
24. Разделы второго уровня политики информационной безопасности.
25. Определение и оценка рисков. Рискообразующие факторы.
26. ISO/IEC 27005:2011 управление рисками ИБ.
27. Структура информационного риска. Понятие «Риск информационной безопасности».
28. Методика анализа риска информационной безопасности. Обработка рисков информационной безопасности.
29. Процесс «управление рисками» в СУИБ.
30. ГОСТ Р ИСО/МЭК 27005-2010 – управление рисками.
31. Место управления рисками информационной безопасности в структуре управления операционными рисками организации.
32. Место управления рисками информационной безопасности в структуре управления информационной безопасностью организации.
33. Цель, задачи и типовая структура департамента информационной безопасности предприятия.
34. Содержание и основные направления процесса управления информационной безопасностью в рамках концепции ITSM.

35. Этапы процесса Управления Информационной Безопасностью предприятия в рамках концепции ITSM.
36. К каким процессам организации может быть применена циклическая модель PDCA?
37. В чем состоят основные преимущества использования циклической модели PDCA?
38. Стадии жизненного цикла политики ИБ?
39. В чем состоят основные различия и сходства стандартов ISO/IEC 27001 и ITU-T X.1051?
40. Как оценивается ИБ ИТ согласно стандартам ISO/IEC 1548 и 18045 и идентичных им ГОСТ Р ИСО/МЭК.
41. Основные направления аудита информационной безопасности на предприятии.
42. Стандарты и практики аудита информационной безопасности.
43. Международный стандарт ISO 19011.
44. Методы организации, подготовки и проведения аудита информационной безопасности.
45. Обработка результатов аудита.
46. Понятие «независимая оценка» состояния информационной безопасности организации.
47. Место аудита информационной безопасности в структуре управления информационной безопасностью организации.
48. Отраслевые стандарты в области управления ИБ.
49. Основные направления процессов реагирования на чрезвычайные ситуации (инциденты) в рамках системы управления информационной безопасностью предприятия.
50. Процедура реагирования на чрезвычайные ситуации (инциденты).
51. Тенденции развития ИБ-рынка в Российской Федерации.

5.4. Примерные базовые вопросы для тестовой формы контроля и дополнительной самостоятельной проверки знаний студентов

5.4.1. Основные направления развития менеджмента в сфере информационной безопасности.
5.4.2. Структура государственных органов, реализующих функции управления информационной безопасностью на государственном уровне.
5.4.3. Функции управления информационной безопасностью.
5.4.4. Разработка государственных стандартов, относящихся к организации и технологиям защиты.
5.4.5. Осуществление международного сотрудничества в сфере защиты информации
5.4.6. Основные направления менеджмента информационной безопасности на уровне предприятия.
5.4.7. Структура политики информационной безопасности.
5.4.8. Структура первого уровня политики информационной безопасности.
5.4.9. Разделы второго уровня политики информационной безопасности.
5.4.10. Определение и оценка рисков. Рискообразующие факторы.
5.4.11. Структура информационного риска. Понятие «Риск информационной безопасности».
5.4.12. Примеры современных технологий защиты информации, основанных на различных базовых сервисах, для механизмов и инструментов защиты информации
5.4.13. Методика анализа риска информационной безопасности. Обработка рисков
5.4.14. Процесс «Управление рисками информационной безопасности».
5.4.15. Место управления рисками информационной безопасности в структуре управления операционными рисками организации.
5.4.16. Место управления рисками информационной безопасности в структуре управления информационной безопасностью организации.
5.4.17. Цель, задачи и типовая структура департамента информационной безопасности предприятия.
5.4.18. Содержание и основные направления процесса управления информационной безопасностью в рамках концепции ITSM.
5.4.19. Этапы процесса Управления Информационной Безопасностью предприятия в рамках концепции ITSM.
5.4.20. Основные направления аудита информационной безопасности на предприятии.

5.4.21. Стандарты и практики аудита информационной безопасности. Международный стандарт ISO 19011
5.4.22. Методы организации, подготовки и проведения аудита информационной безопасности. Обработка результатов аудита.
5.4.23. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности.
5.4.24. Понятие «независимая оценка» состояния информационной безопасности организации. Место аудита информационной безопасности в структуре управления информационной безопасностью организации.
5.4.25. Основные направления процессов реагирования на чрезвычайные ситуации (инциденты) в
5.4.26. рамках системы управления информационной безопасностью предприятия.
5.4.27. Процедура реагирования на чрезвычайные ситуации (инциденты).
5.4.28. Глобальные ИТ-компании в сфере информационной безопасности.
5.4.29. Основные направления, задачи и функции управления информационной безопасностью на уровне крупных поставщиков информационных систем.
5.4.30. Основные направления внешней организационной работы компании в сфере информационной безопасности.
5.4.31. Основные направления внутренней организационной работы компании в сфере информационной безопасности.
5.4.32. Содержание, основные направления управления информационной безопасностью на государственном уровне.

6. Методические указания для обучающихся по освоению дисциплины
Инновационные образовательные технологии

Вид образовательных технологий, средств передачи знаний, формирования умений и практического опыта	№ темы / тема лекции	№ практического (семинарского) занятия /наименование темы	№ лабораторной работы / цель
Слайд-лекции	Тема 1. Концепция управления информационной безопасностью. Базовая терминология.		
Слайд-лекции	Тема 2. Стандартизация систем и процессов управления информационной безопасностью.		
Лекция-дискуссия	Тема 3.Политика информационной безопасности.		
Слайд-лекции	Тема 4. Управление и система управления информационной безопасностью.		

В начале семестра студентам необходимо ознакомиться с технологической картой дисциплины, выяснить, какие результаты освоения дисциплины заявлены (знания, умения, практический опыт). Для успешного освоения дисциплины студентам необходимо выполнить задания, предусмотренные рабочей учебной программой дисциплины и пройти контрольные точки в сроки, указанные в технологической карте (раздел 11). От качества и полноты их выполнения будет зависеть уровень сформированности компетенции и оценка текущей успеваемости по дисциплине. По

итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации, если это предусмотрено технологической картой дисциплины. Списки учебных пособий, научных трудов, которые студентам следует прочесть и законспектировать, темы практических занятий и вопросы к ним, вопросы к зачету и другие необходимые материалы указаны в разработанном для данной дисциплины учебно-методическом комплексе.

Основной формой освоения дисциплины является контактная работа с преподавателем - лекции, лабораторные работы, консультации, в том числе проводимые с применением дистанционных технологий.

По дисциплине часть тем (разделов) изучается студентами самостоятельно. Самостоятельная работа предусматривает подготовку к аудиторным занятиям, выполнение заданий (письменных работ, творческих проектов и др.) подготовку к промежуточной аттестации.

На лекционных занятиях вырабатываются навыки и умения обучающихся по применению полученных знаний в конкретных ситуациях, связанных с будущей профессиональной деятельностью. По окончании изучения дисциплины проводится экзамен.

Регулярное посещение аудиторных занятий не только способствует успешному овладению знаниями, но и помогает организовать время, т.к. все виды учебных занятий распределены в семестре планомерно, с учетом необходимых временных затрат.

6.1. Методические указания для обучающихся по освоению дисциплины на лабораторных работах

Лабораторные работы по дисциплине учебным планом не предусмотрены.

6.2. Методические указания для выполнения контрольных работ

Контрольные работы по дисциплине учебным планом не предусмотрены.

6.3. Методические указания для выполнения курсовых работ (проектов)

Курсовые работы по дисциплине учебным планом не предусмотрены.

7. Паспорт фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (экзамен)

Фонды оценочных средств, позволяющие оценить уровень сформированности компетенций и результаты освоения дисциплины, представлены следующими компонентами: направление подготовки 10.03.01 «Информационная безопасность»

Код оцениваемой компетенции	Тип контроля	Вид контроля	Количество элементов
ОПК-5 ОПК-7	текущий	устный опрос / письменный ответ	9/3 9/3
ОПК-5, ОПК-7	промежуточный	компьютерный тест	80

7.1. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
Знает: ***ОПК-5*** нормативные акты и стандарты в области управления информационной безопасностью ***ОПК-7*** принципы построения информационных систем; принципы организации информационных систем	***ОПК-5*** Развернутый ответ на вопрос с приведением практических примеров: - что такое система управления, основанная на процессном подходе? Подготовить обзор с использование Интернет на тему: - в чем отличие понятий «управление» и «менеджмент»? Краткий письменный ответ на вопрос: - почему информация – это стратегический ресурс?

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
в соответствии с требованиями по защите информации	***ОПК-7*** Развернутый ответ на вопрос с приведением практических примеров: - к каким процессам организации может быть применена циклическая модель PDCA? Подготовить обзор с использование Интернет на тему: - какую роль играют процессы в терминах системного подхода к организации? Краткий письменный ответ на вопрос: - что такое метод управления? Развернутый ответ на вопрос с приведением практических примеров: - в чем состоят основные преимущества использования циклической модели PDCA? Подготовить обзор с использование Интернет на тему: - состояние современных информационных факторов угроз личности, общества, государства и субъектам хозяйствования? Краткий письменный ответ на вопрос: - обобщенная иллюстрация понятия «процесс»?
Умеет: ***ОПК-5*** выполнять планирование, идентификацию и анализ рисков, моделировать риски, проводить мониторинг. ***ОПК-7*** анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах.	***ОПК-5*** Развернутый ответ на вопрос с приведением практических примеров: - в чем различие политик, стандартов, правил и процедур ОИБ? Подготовить обзор с использование Интернет на тему: - для чего разрабатываются организационные (административные)? Краткий письменный ответ на вопрос: - что понимают под ПолИБ в широком и узком смыслах? ***ОПК-7*** Развернутый ответ на вопрос с приведением практических примеров: - стадии жизненного цикла ПолИБ? Подготовить обзор с использование Интернет на тему: - в чем состоят основные различия и сходства стандартов ISO/IEC 27001 и ITU-T X.1051? Краткий письменный ответ на вопрос: - основные идеи руководства по аудиту СУИБ? Развернутый ответ на вопрос с приведением практических примеров: - как оценивается ИБ ИТ согласно стандартам ISO/IEC 1548 и 18045 и идентичных им ГОСТ Р ИСО/МЭК? Подготовить обзор с использование Интернет на тему: - что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла? Краткий письменный ответ на вопрос: - дайте определение «процесс управления ИБ» организации?
Имеет практический опыт: ***ОПК-5*** управления информационной безопасность предприятия в условиях	***ОПК-5*** Развернутый ответ на вопрос с приведением практических примеров: - правовое обеспечение информационной безопасности (ИБ)?

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
применения современных информационных технологий. ***ОПК-7*** анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации; принятие мер защиты информации при выявлении новых угроз безопасности информации; уточнения модели угроз безопасности информации автоматизированной системы.	Подготовить обзор с использование Интернет на тему: - модели организационного управления ИБ? Краткий письменный ответ на вопрос: - служба ИБ организации? ***ОПК-7*** Развернутый ответ на вопрос с приведением практических примеров: - политика информационной безопасности? Подготовить обзор с использование Интернет на тему: - организационное обеспечение ИБ? Краткий письменный ответ на вопрос: - содержание частных политик ИБ? Развернутый ответ на вопрос с приведением практических примеров: - управление конфигурациями, изменениями и обнавлениями? Подготовить обзор с использование Интернет на тему: - стратегии построения и внедрения СУИБ? Краткий письменный ответ на вопрос: - жизненный цикл политики ИБ?

7.2. Методические рекомендации к определению процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Рабочая учебная программа дисциплины содержит следующие структурные элементы:

- перечень компетенций, формируемых в результате изучения дисциплины с указанием этапов их формирования в процессе освоения образовательной программы;

- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (далее–задания). Задания по каждой компетенции, как правило, не должны повторяться.

Требования по формированию задания на оценку ЗНАНИЙ:

- обучающийся должен воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты;

- применяются средства оценивания компетенций: тестирование, вопросы по основным понятиям дисциплины и т.п.

Требования по формированию задания на оценку УМЕНИЙ:

- обучающийся должен решать типовые задачи (выполнять задания) на основе воспроизведения стандартных алгоритмов решения;

- применяются следующие средства оценивания компетенций: простые ситуационные задачи (задания) с коротким ответом или простым действием, упражнения, задания на соответствие или на установление правильной последовательности, эссе и другое.

Требования по формированию задания на оценку навыков и (или) ОПЫТА ДЕЯТЕЛЬНОСТИ:

- обучающийся должен решать усложненные задачи (выполнять задания) на основе приобретенных знаний, умений и навыков, с их применением в определенных ситуациях;

- применяются средства оценивания компетенций: задания требующие многошаговых решений как в известной, так и в нестандартной ситуациях, задания, требующие поэтапного решения и развернутого ответа, ситуационные задачи, проектная деятельность, задания расчетно-графического типа. Средства оценивания компетенций выбираются в соответствии с заявленными результатами обучения по дисциплине.

Процедура выставления оценки доводится до сведения обучающихся в течение месяца с начала изучения дисциплины путем ознакомления их с технологической картой дисциплины, которая является неотъемлемой частью рабочей учебной программы по дисциплине.

В результате оценивания компетенций на различных этапах их формирования по дисциплине студенту начисляются баллы по шкале, указанной в рабочей учебной программе по дисциплине.

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Успешность усвоения дисциплины характеризуется качественной оценкой на основе листа оценки сформированности компетенций, который является приложением к зачетно-экзаменационной ведомости при проведении промежуточной аттестации по дисциплине.

Критерии оценивания компетенций

Компетенция считается сформированной, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует *повышенному уровню* сформированности компетенции.

Компетенция считается сформированной, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует *пороговому уровню* сформированности компетенции.

Компетенция считается несформированной, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет практические работы, не демонстрирует необходимых умений, доля невыполненных заданий, предусмотренных рабочей учебной программой составляет 55 %, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует *допороговому уровню*.

Шкала оценки уровня освоения дисциплины

Качественная оценка может быть выражена: в процентном отношении качества усвоения дисциплины, которая соответствует баллам, и переводится в уровневую шкалу и оценки «отлично» / 5, «хорошо» / 4, «удовлетворительно» / 3, «неудовлетворительно» / 2, «зачтено», «не зачтено». Преподаватель ведет письменный учет текущей успеваемости студента в соответствии с технологической картой по дисциплине.

Шкала оценки результатов освоения дисциплины, сформированности компетенций

Шкалы оценки уровня сформированности компетенции (й)		**Шкала оценки уровня освоения дисциплины**		
Уровневая шкала оценки компетенций	*100 бальная шкала, %*	*100 бальная шкала, %*	*5-балльная шкала, дифференцированная оценка/балл*	*недифференцированная оценка*
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
пороговый	61-85,9	70-85,9	«хорошо» / 4	зачтено
		61-69,9	«удовлетворительно» / 3	зачтено
повышенный	86-100	86-100	«отлично» / 5	зачтено

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Списки основной литературы

1. Баранова, Е. К. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - Документ Bookread2. - М. : РИОР [и др.], 2016. - 321 с. - Режим доступа: http://znanium.com/bookread2.php?book=495249

2. Информатика для экономистов [Электронный ресурс] : учеб. для вузов по направлению 38.03.01 (080100) "Экономика" и 38.03.02 (080200) "Менеджмент" / С. А. Балашова [и др.] под общ. ред. В. М. Матюшка. - 2-е изд., перераб. и доп. - Документ Bookread2. - М. : ИНФРА-М, 2016. - 459 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=541005

3. Олифер, В. Г. Безопасность компьютерных сетей [Текст] / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия -Телеком, 2016. - 644 с.

4. Курило А.П., Милославская Н.Г. Сенаторов М.Ю. Толстой А.И. Основы управления информационной безопасностью [Текст] Учебное пособие для вузов. -2-е изд., испр. - М.: Горячая линия – Телеком, 2016. - 244 с.

5. Учебно-методический комплекс по дисциплине "Информационная безопасность" [Электронный ресурс] : для студентов направления подгот. 38.03.05 "Бизнес-информатика" и 09.03.03 "Приклад. информатика" / Поволж. гос. ун-т сервиса (ФГБОУ ВПО "ПВГУС"), Каф. "Приклад. информатика в экономике" ; сост. В. С. Марченко. - Документ Adobe Acrobat. - Тольятти : ПВГУС, 2015. - 1,83 МБ, 116 с. - Режим доступа: http://elib.tolgas.ru

6. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ Bookread2. - М. : ФОРУМ [и др.], 2018. - 592 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=937502

Списки дополнительной литературы

7. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Текст] : учеб. пособие для вузов по специальностям "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" / А. А. Афанасьев [и др.] под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. - М. : Горячая линия - Телеком, 2009. - 550 с.

8. Бабаш, А. В. Информационная безопасность. Лабораторный практикум [Текст] : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - М. : КноРус, 2012. - 131 с.

9. Белоножкин, В. И. Информационные аспекты противодействия терроризму [Текст] / В. И. Белоножкин, Г. А. Остапенко. - М. : Горячая линия - Телеком, 2009. - 112 с.

10. Введение в информационную безопасность [Текст] : учеб. пособие для вузов / А. А. Малюк [и др.] под ред. В. С. Горбатова. - М. : Горячая линия - Телеком, 2011. - 288 с.

11. Гашков, С. Б. Криптографические методы защиты информации [Электронный ресурс] : учеб. пособие для вузов по направлениям "Приклад. математика и информатика" и "Информ. технологии" / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Документ Adobe Acrobat. - М. : Академия, 2010. - 41,4 МБ, 299 с. : ил. - Режим доступа: http://elib.tolgas.ru

12. Городов, О. А. Информационное право [Текст] : учебник / О. А. Городов. - М. : Проспект, 2009. - 242 с.

13. Грушо, А. А. Теоретические основы компьютерной безопасности [Текст] : учеб. пособие для вузов по специальности "Информ. безопасность" / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М. : Академия, 2009. - 268 с.

14. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Текст] : учеб. пособие для вузов по специальностям направления подгот. "Информ. безопасность вычисл. автоматизир. и телекоммуникац. систем", "Информ. безопасность" / П. Н. Девянин. - М. : Горячая линия - Телеком, 2012. - 320 с.

15. Ищейнов, В. Я. Защита конфиденциальной информации [Текст] : учеб. пособие для вузов по специальностям "Орг. и технология защиты информ.", "Комплексная защита объектов информ." / В. Я. Ищейнов, М. В. Мецатунян. - М. : ФОРУМ, 2013. - 256 с.

16. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для вузов по специальности "Информ. системы и технологии" / В. П. Мельников, А. М. Петраковпод ред. С. А. Клейменова. - 6-е изд., стер. - М. : Академия, 2012. - 336 с.

17. Расторгуев, С. П. Основы информационной безопасности [Текст] : учеб. пособие для вузов по специальностям "Компьютерная безопасность", "Информ. безопасность телекоммуникац. систем" / С. П. Расторгуев. - М. : Академия, 2007. - 187 с.

18. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие для вузов по направлению "Информатика и вычисл. техника" / П. Б. Хорев. - 3-е изд., стер. - М. : Академия, 2007. - 255 с.

8.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины

Интернет-ресурсы

1. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. - Режим доступа: http://elib.tolgas.ru/. - Загл. с экрана.

2. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим дос Режим доступа: http://znanium.com/. – Загл. с экрана.

3. Электронно-библиотечная система Лань [Электронный ресурс]. - Режим доступа: https://e.lanbook.com/books. - Загл. с экрана.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Краткая характеристика применяемого программного обеспечения

№ п/п	Программный продукт	Характеристика	Назначение при освоении дисциплины
1	Интернет браузер	Прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; а также для решения других задач.	Поиск информации в сети «Интернет»
2	Пакет MS Office Professional	Пакет приложений, содержащий программное обеспечение для работы с различными типами документов: текстами, электронными таблицами, базами данных и др. Microsoft Office является сервером OLE-объектов и его функции могут использоваться другими приложениями, а также самими приложениями Microsoft Office.	Разработка баз данных, проведение расчетов, оформление текстовых документов, подготовка презентаций
3	Microsoft Visio	Графический редактор моделей	Построение графических моделей
4	СПИС «Консультант Плюс»	Справочно-поисковая система	Поиск нормативно-справочной информации
5	Secret Net	Система защиты информации	Средство защиты информации от несанкционированного доступа
6	vipNet (client, coordinator, administrator)	Система защиты информации	Средство защиты информации
7	Антивирус Касперского	Система защиты информации	Средство защиты информации и оборудования
8	КриптоПро	Система защиты информации	Средство защиты информации
9	x-spider	Система защиты информации	Средство и система защиты информации

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа используются специальные помещения – учебные аудитории, укомплектованные специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации.

Для проведения лабораторных работ используется лаборатория «Аудитория информационных технологий, информатики и методов программирования», оснащенная лабораторным оборудованием различной степени сложности

Для текущего контроля и промежуточной аттестации используются специальные помещения – учебные аудитории, укомплектованные специализированной мебелью, и (или) компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета.

Для самостоятельной работы обучающихся используются специальные помещения – учебные аудитории для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета.

11. Примерная технологическая карта дисциплины Основы управления информационной безопасностью

Институт (факультет) экономики
кафедра «Прикладная информатика в экономике»
преподаватель _____ направление подготовки 10.03.01 «Информационная безопасность»
направленности (профиля) «Организация и технология защиты информации»
(7-ой семестр)

№	Виды контрольных точек	Кол-во контр. точек	Кол-во баллов за 1 контр. точку	График прохождения контрольных точек																зач. неделя
				сентябрь				октябрь				ноябрь				декабрь				
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1	Обязательные контрольные точки																			
1.1	Посещение лекций	10	2	+	+	+	+	+		+		+		+		+	+			20
1.2	Посещение практических занятий	10	2		+		+		+	+	+		+	+	+	+	+	+		20
1.3	Выполнение практических работ	10	4		+		+		+		+		+	+	+	+	+	+		40
2	Дополнительные задания																			
2.1	Промежуточное тестирование	1	20										+							20
2.2	Выполнение индивидуальной работы	1	20										+							20
3	Творческие задания																			
3.1	Подготовка статьи на конференцию, форум	1	20						+											20
3.2	Написание научно-исследовтельской работы		20													+				20
3.3	Участие в форумах, конференциях		до 30																	30
	Общий рейтинг по дисциплине																			100
	Форма контроля																			

Институт (факультет) экономики
кафедра «Прикладная информатика в экономике»
преподаватель _____ направление подготовки 10.03.01 «Информационная безопасность»
направленность (профиль) «Организация и технология защиты информации (8-ой семестр)

№	Виды контрольных точек	Кол-во контр. точек	Кол-во баллов за 1 контр. точку	График прохождения контрольных точек																зач. неделя
				февраль				март				апрель				май				
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1	Обязательные контрольные точки																			
1.1	Посещение лекций	9	2	+	+	+	+	+		+		+		+		+				18
1.2	Посещение практических занятий	6	4						+		+		+		+	+		+		24
1.3	Выполнение практических работ	6	6				+		+		+		+			+		+		36
2	Дополнительные задания																			
2.1	Выполнение индивидуальной работы	1	20										+							20
2.2	Промежуточное тестирование	1	20										+							20
3	Творческие задания																			
3.1	Подготовка доклада на конференцию	2	12						+							+				24
3.2	Написание научно-исследовтельской работы		22													+				22
3.3	Участие в форумах, конференциях		до 30																	30
	Общий рейтинг по дисциплине																			100
	Форма контроля																			экзамен