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
Информационно-аналитическая деятельность по обеспечению комплексной безопасности
наименование дисциплины (модуля, междисциплинарного курса)

для студентов направления подготовки 10.03.01 «Информационная безопасность»
направленности (профиля) «Организация и технология защиты информации»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине Информационно-аналитическая деятельность по обеспечению комплексной безопасности 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 «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» разработана в соответствии с Федеральным государственным образовательным стандартом направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Минобрнауки РФ от 1 декабря 2016 г. N 1515.

Составил к.э.н.,доцент Филиппова О.А.
(ученая степень, звание, Ф.И.О.)

Согласовано Директор научной библиотеки _____ В.Н.Еремина

Согласовано Начальник управления информатизации _____В.В.Обухов

Рабочая программа утверждена на заседании кафедры «Прикладная информатика в экономике»
(наименование кафедры)

Протокол № 12 от «22» июня 2018г.

И.о. заведующего кафедрой _____ д.э.н., профессор Бердников В.А._____
(подпись) (ученая степень, звание, Ф.И.О.)

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:

- формирование профессиональной направленности у студентов и овладение системой знаний в области применения информационно-аналитической деятельности по обеспечению комплексной безопасности.

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

- способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;
- 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.

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины у обучающихся формируются следующие компетенции:

Код компетенции	Наименование компетенции
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

1.4. Перечень планируемых результатов обучения по дисциплине

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
Знает: значение информации в развитии современного общества и возможности информационных технологий для поиска и обработки информации (ОПК-4) методы определения угроз безопасности и выявления информационных ресурсов, подлежащих защите (ОПК-7)	Лекции, практические работы	Собеседование, защита практических работ, индивидуальное задание
Умеет: применять информационные технологии для поиска и	Лекции, практические работы	Собеседование, защита практических работ, индивидуальное задание

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
обработки информации (ОПК-4) анализировать структуру и содержание информационных процессов и особенностей функционирования объекта защиты с целью выявления угроз информационной безопасности (ОПК-7)		
Имеет практический опыт: применения информационных технологий для поиска и обработки информации (ОПК-4) определения угроз безопасности для информационных ресурсов, подлежащих защите и пути их снижения (ОПК-7)	Лекции, практические работы	Собеседование, защита практических работ, индивидуальное задание

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части направления подготовки 10.03.01 «Информационная безопасность». Ее освоение осуществляется в 6 семестре (очное отделение), 7 и 9 семестре (очно-заочное отделение).

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код и наименование компетенций
	Предшествующие дисциплины (практики)	
	Проектирование информационных систем	ОПК-4, способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
	Информационные системы и технологии	ОПК-4, способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
	Защита и обработка конфиденциальных документов	ПК-1, способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-3, способностью администрировать подсистемы информационной безопасности объекта защиты

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

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

Виды занятий	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Итого часов Зачетных единиц	216 ч. 6 з.е.	216 ч. 6 з.е	-
Лекции (час)	32	10	-
Практические (семинарские) занятия (час)	64	12	-
Лабораторные работы (час)	-	-	-
Самостоятельная работа (час)	93	194	-
Курсовой проект (работа) (+,-)	+	+	-
Контрольная работа (+,-)	-		-
Экзамен, семестр /час.	- 6 (27 час.)	9 (9час.)	-
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 (семинарские) занятия, час	Лабораторные работы, час	Самостоятельная работа, час	
1	**Тема 1. Введение в информационно-аналитическую деятельность** Основное содержание: 1.1. Основные понятия информационно-аналитической деятельности. Цели и задачи. Объект, предмет информационно-аналитической деятельности по обеспечению комплексной безопасности (ИАДКД). 1.2. Специфика информационно-аналитической деятельности. Основные принципы и технологии реализации. Терминология. 1.3. Технологический цикл информационно-аналитической деятельности. 1.4. ГОСТ Р 56875-2016 Информационные технологии (ИТ). Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий 1.5. Требования к построению информационно-аналитической деятельности по обеспечению комплексной безопасности (ИАДКД). 1.6. Информационно-аналитическая система "АРИОН" и ее функциональные возможности.	12/2	24/2	-/-	24/55	устный опрос, защита практических работ, индивидуальное задание
2	**Тема 2. Планирование и проектирование информационно-аналитической деятельности по обеспечению комплексной безопасности** Основное содержание: 2.1 Системный подход к организации информационно-аналитической деятельности	12/4	16/2	-/-	24/65	устный опрос, защита практических работ, индивидуальное задание

№ п/п	Раздел дисциплины	Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в академических часах)				Средства и технологии оценки
		Лекции, час	Практические (семинарские) занятия, час	Лабораторные работы, час	Самостоятельная работа, час	
	2.2 Сущность и задачи комплексной системы безопасности. Функциональность. 2.3 Определение состава защищаемой информации. Информационные активы. 2.4 Источники, способы и результаты дестабилизирующего воздействия на информацию. Объекты оценки. 2.5 Анализ информативности источников. Оценка полноты, непротиворечивости и достоверности информации. 2.6 Технология создания информационно-аналитических документов. 2.7 Отчетные документы ИАДКБ					
3	**Тема 3. Организация информационно-аналитической деятельности по обеспечению комплексной безопасности в бизнес-структурах** Основное содержание: 3.1 Функциональная модель безопасности предприятия. 3.2 Нормативные требования к защите информационных ресурсов предприятия и правам доступа пользователей к ИАДКБ 3.3 Нормативные требования уровню защищенности и способам поддержки информационных ресурсов 3.4 Структура системы информационно-аналитической деятельности по обеспечению комплексной безопасности 3.5 Разработка технического задания (ТЗ) на построение ИАДКБ. 3.6 Разработка Профилей защиты (ПЗ) информационной безопасности в соответствии с ГОСТ Р 57628-2017	8/4	24/8	-/-	49/74	устный опрос, защита практических работ, индивидуальное задание
	Промежуточная аттестация по дисциплине 6 семестр (о/о), 9 семестр (з/о)	32/10	64/12	-/-	93/194	**Экзамен (27/9)**

4.2.Содержание практических (семинарских) занятий

№	Наименование практических работ	Обьем часов	Наименование темы дисциплины
	6/9 семестр*		
1	Практическая работа № 1. Изучение специфики информационно-аналитической деятельности	4/0	Тема 1 Введение в информационно-аналитическую деятельность
2	Практическая работа № 2. Изучение нормативных документов по организации и обеспечению информационно-аналитической деятельности	4/0	
3	Практическая работа № 3. Изучение требований ГОСТ Р 56875-2016 к построению комплексных систем защиты информации.	4/0	
4	Практическая работа № 4. Требования стандарта ISO/IEC 27000 к построению комплексных систем информационной безопасности	4/0	
5	Практическая работа № 5. Изучение требований стандарта ITIL к разработке Политики ИБ в разрезе информационно- аналитической деятельности	4/2	
6	Практическая работа № 6. Изучение требований нормативных документов к оценке рисков информационно-аналитической деятельности по обеспечению комплексной безопасности	4/2	
7	Практическая работа № 7. Определение состава защищаемой информации. Обоснование выбора информационных активов в разрезе нормативных требований.	4/0	Тема 2. Планирование и проектирование информационно-аналитической деятельности по обеспечению комплексной безопасности
8	Практическая работа № 8. Анализ источников, способов и результатов дестабилизирующего воздействия на информацию.	4/2	
9	Практическая работа № 9. Изучение возможных объектов оценки и формирование их перечня, с учетом ответственных лиц.	4/0	
10	Практическая работа № 10. Построение шаблонов Карт контроля доступа к объектам оценки информационных активов в соответствии с требованиями ГОСТ Р ИСО/МЭК 27000.	4/2	
11	Практическая работа № 11. Изучение нормативных требований к составу и содержанию системы ИАДКД для конкретной организации в соответствии с требованиями ГОСТ Р 57628-2017	4/0	Тема 3. Организация информационно-аналитической деятельности по обеспечению комплексной безопасности в бизнес-структурах
12	Практическая работа № 12. Изучение особенностей построения типовой структуры ИАДКД для конкретного предприятия (организации).	4/0	
13	Практическая работа № 13. Разработка ТЗ на построение ИАДКД для конкретного предприятия (организации).	4/0	
14	Практическая работа № 14. Разработка структуры и функционала ИАДКД на примере конкретной организации	4/2	

№	Наименование практических работ	Обьем часов	Наименование темы дисциплины
15	Практическая работа № 15. Разработка перечня информационных активов и обоснование выбора объектов оценки	4/2	
16	Практическая работа № 16. Построение Профилей Защиты информации	4/2	
	Итого за 6/9* семестр	**64/12**	

*** - заочная форма обучения**

4.3.Содержание лабораторных работ

Лабораторные работы по дисциплине учебным планом не предусмотрены

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Технологическая карта самостоятельной работы студента

Код реализуемой компетенции	Вид деятельности студентов (задания на самостоятельную работу)	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов
1	2	3	4	5
ОПК-4, ОПК-7	Выполнить и защитить курсовую работу в соответствии с темой индивидуального задания	Курсовая работа	Опрос, тестирование	93/194
			Итого за 6/9 семестр	93/194

Рекомендуемая литература: 1, 3, 5.

Содержание заданий для самостоятельной работы

Темы для выполнения заданий на самостоятельную работу

1. Анализ информативности источников.
2. Оценка полноты, непротиворечивости и достоверности информации.
3. Технология создания аналитических документов.
4. Критерии, параметры ограничения логической непротиворечивости и достоверности информации.
5. Система информационно-аналитического обеспечения в сфере безопасности
6. Особенности архитектуры систем информационно-аналитического обеспечения?
7. Информационно-аналитические центры в РФ, их функции
8. Требования к системам комплексной безопасности по ГОСТ Р ИСО 27000
9. Требования к системам комплексной безопасности по ГОСТ Р 57628-2017
10. Требования к системам комплексной безопасности по ГОСТ Р 56875-2016

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.

Вопросы для самоконтроля

По теме 1

1. Информационно-аналитическое обеспечение деятельности специалистов сфере информационной безопасности
2. Специфика сферы информационной безопасности в контексте аналитической деятельности.
3. Сущность информационно-аналитического обеспечения.
4 Информационно-аналитическое обеспечение деятельности государственных органов в сфере компьютерных преступлений
5. Анализ современного состояния «хакерства» в России и за рубежом:
6. Отличие хакеров и криптоаналитиков.
7. Информационно-аналитическая работа в команде:
8. Современное состояние и проблемы информационно- аналитической деятельности
9. Объект, предмет информационно-аналитической деятельности
комплексной безопасности
10 Что такое информационная безопасность?
11. Как защитить информацию?
12 Какая нормативная база обеспечивает поддержку защиты информации
13. Каковы фундаментальные свойства оцифрованной информации
14. Какие существуют подходы к моделированию угроз информационной безопасности
15 Какие существуют методы и инструменты анализа и контроля информационных рисков
16. Что включает в себя информационно-аналитическая деятельность
17 Каковы требования к системам комплексной безопасности предъявляются по ГОСТ Р ИСО 27000
18. Какие требования к системам комплексной безопасности предъявляются по ГОСТ Р 57628-2017
19. Каковы требования к информационно-аналитической деятельности и к системам комплексной безопасности по ГОСТ Р 56875-2016
20. Дать определение информационно-аналитической деятельности

По теме 2

1. Какую роль играет системный подход организации информационно-аналитической деятельности?
2. Описать сущность и задачи комплексной системы безопасности.
3. Описать требования к функциональности систем информационно-аналитической деятельности.
4. Средства и методы информационно-аналитической деятельности для определение состава защищаемой информации.
5. По какому принципу на предприятии формируются информационные активы.
6. Источники, способы и результаты дестабилизирующего воздействия на информацию.
7. Объекты оценки, как результат информационно-аналитической деятельности.
8. Анализ информативности источников.
9. Оценка полноты, непротиворечивости и достоверности информации.
10.Технология создания информационно-аналитических документов.
11. Отчетные документы информационно-аналитической деятельности комплексной безопасности
12. Особенности планирования информационно-аналитического обеспечения комплексной безопасности.
13. Особенности проектирования информационно-аналитического обеспечения комплексной безопасности.
14. Анализ требований к кадровому ресурсу в области информационно-аналитической деятельности.
15. Описать общий вид Карт контроля доступа к информационным активам.

По теме 3

1 Функциональная модель безопасности предприятия.

2 Нормативные требования к защите информационных ресурсов предприятия и правам доступа пользователей к ИАДКБ
3 Нормативные требования уровню защищенности и способам поддержки информационных ресурсов
4 Структура системы информационно-аналитической деятельности по обеспечению комплексной безопасности
5 Описать нормативные требования к структуре информационно-аналитической деятельностипо обеспечению комплексной безопасности.
6. Дать краткую характеристику Профилю защиты безопасности в организации.
7. Описать алгоритм разработки Профилей защиты (ПЗ) информационной безопасности в соответствии с ГОСТ Р 57628-2017
8. Описать особенности контроля защищенности информационного актива.
9. Описать сущностную характеристику Модели угроз информационной безопасности.
10. Описать состав информационно-аналитической системы обеспечения комплексной информации.

5. 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
Лекция-дискуссия,	Тема 1 Введение в информационно-аналитическую деятельность		
Лекция-дискуссия	Тема 2. Планирование и проектирование информационно-аналитической деятельности по обеспечению комплексной безопасности		
Лекция-дискуссия	Тема 3. Организация информационно-аналитической деятельности по обеспечению комплексной безопасности в бизнес-структурах		

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 (зачету).

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 промежуточная аттестация (зачет).

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

Контрольная работа по дисциплине учебным планом не предусмотрена.

6.3. Методические указания для выполнения курсовых работ (проектов)

Курсовая работа оформляется в соответствии со стандартными требованиями, принятыми в вузе.

Целью курсовой работы является формирование практических навыков по формированию информационно-аналитического обеспечения при организации системы комплексной безопасности

Объем курсовой работы 30-35 листов.

Курсовая работа содержит три части: аналитическую, проектную и экономическую.

Во введении описывается актуальность темы исследования и обоснование выбора предметной области, краткое описание существующей проблемы, возникающей в процессе информационно-аналитической деятельности, объект и предмет исследования, цели и задачи курсовой работы, нормативная и информационная база.

В качестве **нормативной базы** исследования рекомендовано изучить требования таких нормативных документов, как ГОСТ Р ИСО 27000, ГОСТ Р 57628-2017, ГОСТ Р 56875-2016, в которых описаны требования, предъявляемые как к процессу информационно-аналитической деятельности, так и к процессам построения систем комплексной безопасности.

В качестве **информационной базы** рекомендовано использовать первичные документы своей организации. выступающей в качестве объекта исследования. Это могут быть различные информационные активы, информационные потоки, документ "Политика ИБ"

В качестве **методической базы** рекомендовано использовать внутривузовские требования и стандарты на оформление курсовых работ.

В аналитической части выполняется анализ существующих подходов к построению информационно-аналитического обеспечения в организации. Организация выбирается самостоятельно на примере своего рабочего места (по профилю получаемой квалификации).

Рекомендовано исследовать схему информационно-аналитического обеспечения в сфере управления (Источник: Нестеров А.К. Информационно-аналитическое обеспечение // Образовательная энциклопедия ODiplom.ru - http://odiplom.ru/lab/informacionno-analiticheskoe-obespechenie.html). Выполнить анализ применяемых концептуальных подходов к информационно-аналитической деятельности и к информационно-аналитическому обеспечению, а также,

принципам, средствам и методам его построения. Заканчивается теоретическая глава краткими выводами о том, какие следует применять инструменты для проектирования информационно-аналитической деятельности для обеспечения комплексной безопасности предприятия (организации).

В проектной части предлагается разработать техническое задание **(ТЗ) на проект информационно-аналитической деятельности по обеспечению комплексной безопасности.** Обязательным условием является построение Профилей Защиты информационных активов, обоснование объектов оценки (ОО) и расчет прогнозируемых уровней риска информационной безопасности. Базовыми нормативными документами для построения Проекта ИАДКБ являются ГОСТ Р 57628-2017, в котором описаны требования к построению Профилей защиты и других результатов информационно-аналитической деятельности, а также ГОСТ 34.602-89 Техническое задание на создание автоматизированной системы.

В экономической части показано обоснование затрат на проектирование и разработку информационно-аналитического обеспечения для систем комплексной безопасности в организации.

В заключении должны быть сформулированы выводы о значимости предлагаемых проектных решений для объекта исследования.

Примерный список тем курсовых работ[1]

1. Проект информационно-аналитической деятельности для систем комплексной безопасности в торговой организации (на примере...)
2. Проект информационно-аналитической деятельности для систем комплексной безопасности в бюджетной организации (на примере...)
3. Проект информационно-аналитической деятельности для систем комплексной безопасности в государственном учреждении (на примере...)
4. Проект информационно-аналитической деятельности для систем комплексной безопасности в производственной системе (на примере...)
5. Проект информационно-аналитической деятельности для систем комплексной безопасности в интегрированной производственной структуре (на примере...)
6. Проект информационно-аналитической деятельности для систем комплексной безопасности в финансово-кредитной организации (на примере...)
7. Проект информационно-аналитической деятельности для систем комплексной безопасности в коммерческой организации (на примере...)

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:

Код оцениваемой компетенции	Тип контроля	Вид контроля	Количество элементов
ОПК-4	текущий	устный опрос	10
ОПК-7	текущий	устный опрос	10
промежуточный (ОПК-4, ОПК-7)		компьютерный тест	80

[1] Тема может быть предложена самостоятельно студентом, после ее утверждения с преподавателем

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: значение информации в развитии современного общества и возможности информационных технологий для поиска и обработки информации (ОПК-4) методы определения угроз безопасности и выявления информационных ресурсов, подлежащих защите (ОПК-7)	**ОПК-4** Краткий письменный ответ на вопросы 1. Первичная обработка информации и ее особенности. 2. Методика информационного поиска. 3. Основные принципы аналитической деятельности. 4. Описать основную нормативную базу, направленную на защиту информационной безопасности 5. Перечислить фундаментальные свойства оцифрованной информации и кратко охарактеризовать каждое из них **ОПК-7** Краткий письменный ответ на вопросы 1.Перечислить подходы к моделированию угроз информационной безопасности 2. Охарактеризовать базовые инструменты анализа и контроля информационных рисков 3. Описать преимущества и недостатки количественной оценки соотношения потерь от угроз безопасности и затрат на создание системы защиты 4.Организация защиты информации в различных направлениях деятельности предприятия (организации). 5. Организация работы службы безопасности предприятия (организации).
Умеет: применять информационные технологии для поиска и обработки информации (ОПК-4) анализировать структуру и содержание информационных процессов и особенностей функционирования объекта защиты с целью выявления угроз информационной безопасности (ОПК-7)	Развернутый письменный ответ на вопросы с приведением практических примеров. **ОПК-4** Применяя стандартные технологии поиска и обработки информации. выполнить: 1. Построить Модель Политики информационной безопасности организации с учетом ее планов развития. 2. Создать типовой документ для организации системы защиты информационной безопасности **ОПК-7** 1. Выполнить анализ информационно-аналитического обеспечения на примере конкретной организации.. 2. Описать структурную схему инфформационно-аналитического обеспенчения организации на трех уровнях управления (операционном, тактическом и стратегическом) 3. Для каждого из уровней выявить угрозы информационной безопасности.
Имеет практический опыт: применения информационных технологий для поиска и обработки информации (ОПК-4) определения угроз безопасности для информационных ресурсов, подлежащих защите и пути их снижения (ОПК-7)	**ОПК-4** 1. Составить перечень используемых технологий поиска информации по запросам и ее аналитической обработки. Выделить два уровня информационно-аналитического обеспечения в сфере управления: 1) Информационный уровень, который заключается в поиске, сборе, хранении, распространении информации; 2) Аналитический уровень, который заключается в обобщении, классификации информации, ее анализе и преобразовании, разработке выводов, предложений,

Результаты освоения дисциплины	**Оценочные средства** (перечень вопросов, заданий и др.)
	рекомендаций и прогнозов. Сделать выводы. **ОПК-7** 1. Выполнить анализ защищенности информационной системы организации на основе выявления уязвимостей и обнаружения вторжений. 2. Выполнить расчет выявленных рисков информационной безопасности. Методику, выбранную для расчета, обосновать. 3. Предложить рекомендации по снижению рисков.

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.

7.3. 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. Баяндин, Н. И. Информационно-аналитическое обеспечение безопасности бизнеса. Деловая разведка [Текст] : учеб. по направлению подгот. "Информ. безопасность" / Н. И. Баяндин. - СПб. : Интермедия, 2016. - 224 с.
2. Варфоломеева, А. О. Информационные системы предприятия [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.03. "Приклад. информатика" и др. экон. специальностям / А. О. Варфоломеева, А. В. Коряковский, В. П. Романов. - 2-е изд., перераб. и доп. - Документ Bookread2. - М. : ИНФРА-М, 2019. - 330 с. - Режим доступа: http://znanium.com/bookread2.php?book=1002067.
3. 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

4. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учеб. пособие для вузов по специальностям "Орг. и технология защиты информ.", "Комплекс. защита объектов информатизации" / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 412 с.
5. 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.
6. Проскурин, В. Г. Защита программ и данных [Текст] : учеб. пособие для вузов по направлению подгот. "Информ. безопасность" (бакалавр) и специальностям: "Компьютер.

безопасность", "Информ. безопасность автоматизир. систем" / В. Г. Проскурин. - М. : Академия, 2012. - 208 с.

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

Интернет-ресурсы

1. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. - Режим доступа: http://elibrary.ru/defaultx.asp. - Загл с экрана

2. Универсальные базы данных East View [Электронный ресурс]. - Режим доступа: http://www.ebiblioteka.ru/. - Загл. с экрана.

3. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. - Режим доступа: http://elib.tolgas.ru/. - Загл. с экрана.
4. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим дос Режим доступа: http://znanium.com/. – Загл. с экрана.
5. 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.	Оформление текстовых документов, подготовка презентаций.

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 практических занятий (занятий семинарского типа), групповых и индивидуальных консультаций используются специальные помещения - учебные аудитории, укомплектованные специализированной мебелью и техническими средствами обучения.

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 Информационно-аналитическая деятельность по обеспечению комплексной безопасности

Институт (факультет) экономики
кафедра «Прикладная информатика в экономике»
преподаватель_____, направление подготовки 10.03.01 «Информационная безопасность»

№	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	10	1	+	+	+	+	+		+		+		+		+		+		10
1.2	Выполнение практических работ	10	5		+	+	+		+		+	+	+		+		+	+		50
1.3	Выполнение курсовой работы	1	30																	30
2	Дополнительные задания																			
2.1	Выполнение индивидуальной работы	1	10													+				10
																				100
	экзамен																			