

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Вабинова Любовь Александровна

Должность: Ректор

Дата подписания: 04.02.2022 15:17:47

Уникальный программный ключ:

c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

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

Кафедра Прикладная информатика в экономике

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

по дисциплине «Основы информационной безопасности»
для студентов направления подготовки 10.03.01 «Информационная безопасность»
направленность (профиль) «Организация и технология защиты информации»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине «Основы информационной безопасности» включена в основную профессиональную образовательную программу направления подготовки 10.03.01 «Информационная безопасность» направленность (профиль) «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 информационной 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: 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:

- формирование профессиональной направленности у студентов и овладение системой знаний в области основ информационной безопасности.

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
ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.
ОПК-7	Способность 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 информационной безопасности»

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
Знает: ОК-5 социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.	Лекции, лабораторные работы	собеседование, выполнение лабораторных работ

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
ОПК-7 угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты, обладает способностью определять информационные ресурсы, подлежащие защите,		
Умеет: ОК-5 понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. ОПК-7 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.	Лекции, лабораторные работы, индивидуальные задания, использование интернет ресурсов.	собеседование, выполнение лабораторных работ, подготовка рефератов, докладов
Имеет практический опыт: ОК-5 в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики, развил способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности ОПК-7 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.	Лекции, лабораторные работы, самостоятельная работа, использование интернет ресурсов.	собеседование, выполнение лабораторных работ 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 4 семестре у студентов дневной формы обучения и в 5 семестре у студентов очно-заочной форме обучения.

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код и наименование компетенций
	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)	
	Организационное и правовое обеспечение информационной безопасности	ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности; ОПК-5 способностью использовать нормативные правовые акты в профессиональной деятельности.

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	144 ч.	144	—
Зачетных единиц	4 з.е.	4 з.е.	—
Лекции (час)	20	4	—
Практические (семинарские) занятия (час)	-	-	-
Лабораторные работы (час)	30	10	-
Самостоятельная работа (час)	67	121	-
Курсовой проект (работа) (+,-)	-	-	-
Контрольная работа (+,-)	-	-	-
Экзамен, семестр /час.	4 / 27	5 / 9	-
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	Практи- ческие занятия, час	Лабораторные работы, час	Самостоятельная работа, час	
1	Тема 1. Концепция информационной безопасности. Защита. Виды противников или нарушителей	2/0,3/-	-/-/-	2/1/-	11/12/-	устный опрос, разбор лабораторных работ, индивидуальное задание
2	Тема 2. Анализ способов нарушений информационной безопасности.	2/0,3/-	-/-/-	4/1/-	11/12/-	устный опрос, обсуждение лабораторных работ, индивидуальное задание
3	Тема 3. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	2/0,5/-	-/-/-	2/1/-	11/12/-	устный опрос, обсуждение лабораторных работ, индивидуальное задание
4	Тема 4. Понятия о видах компьютерных вирусов и тренды их развития.	2/0,5/-	-/-/-	4/1/-	11/13/-	устный опрос, обсуждение лабораторных работ, индивидуальное задание
5	Тема 5. Методы криптографии.	2/0,5/-	-/-/-	4/1/-	11/12/-	устный опрос, обсуждение лабораторных работ, индивидуальное задание
6	Тема 6. Основные положения теории информационной безопасности информационных систем.	2/0,3/-	-/-/-	2/1/-	11/12/-	устный опрос, обсуждение лабораторных работ, индивидуальное задание
7	Тема 7. Построение комплексных систем защиты информации. Использование защищенных компьютерных систем.	2/0,5/-	-/-/-	4/1/-	11/12/-	устный опрос, обсуждение лабораторных работ, индивидуальное задание
8	Тема 8. Модели безопасности и их применение	2/0,3/-	-/-/-	2/1/-	11/12/-	устный опрос, обсуждение

						лабораторных работ, индивидуальное задание
9	Тема 9. Стандарты информационного обмена и информационная безопасность в санкционных условиях функционирования в России глобальных сетей.	2/0,5/-	-/-/-	4/1/-	11/12/-	устный опрос, обсуждение лабораторных работ, индивидуальное задание
10	Тема 10. Место информационной безопасности экономических систем в Национальной безопасности страны.	2/0,3/-	-/-/-	2/1/-	17/12/-	устный опрос, обсуждение лабораторных работ, индивидуальное задание
	Промежуточная аттестация по дисциплине	20/4/-	-/-/-	30/10/-	67/121/-	экзамен

4.2. Содержание практических (семинарских) занятий

Практические (семинарские) занятия по дисциплине учебным планом не предусмотрены

4.3. Содержание лабораторных работ

Лабораторные работы обеспечивают: формирование умений и навыков обращения с техническими средствами, демонстрацию применения теоретических знаний на практике, закрепление и углубление теоретических знаний, контроль знаний и умений в формулировании выводов, развитие интереса к изучаемой дисциплине.

Применение лабораторных работ позволяет вовлечь в активную работу всех обучающихся группы и сформировать интерес к изучению дисциплины.

Самостоятельный поиск ответов на поставленные вопросы и задачи в ходе лабораторной работы приобретают особую значимость в восприятии, понимании содержания дисциплины.

Изученный на лекциях материал лучше усваивается, лабораторные работы демонстрируют практическое их применение.

№	Наименование лабораторных работ	Объем часов	Наименование темы дисциплины
	4 семестр		
1	Лабораторная работа 1. Источники угроз и уязвимые места информационных систем, виды противников.	8/2/-	Тема 1. Концепция информационной безопасности. Защита. Виды противников или нарушителей. Тема 2. Анализ способов нарушений информационной безопасности. Тема 3. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
2	Лабораторная работа 2. Компьютерные вирусы.	4/2/-	Тема 4. Понятия о видах компьютерных вирусов и тренды их развития.
3	Лабораторная работа 3. Криптография.	6/2/-	Тема 5. Методы криптографии. Тема 6. Основные положения теории информационной безопасности информационных систем.
4	Лабораторная работа 4. Стандарты информационной	6/2/-	Тема 8. Модели безопасности и их применение. Тема 9. Стандарты информационного обмена и

	безопасности построение системы защиты информации.		информационная безопасность в санкционных условиях функционирования в России глобальных сетей.
5	Лабораторная работа 5. Правовые аспекты информационной защиты.	6/2/-	Тема 7. Построение комплексных систем защиты информации. Использование защищенных компьютерных систем. Тема 10. Место информационной безопасности экономических систем в национальной безопасности страны.
	Итого за 4/5 семестр	30/10/-	
	Итого	30/10/-	

5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студента является важным фактором успешного изучения дисциплины «Сети и системы передачи информации». Домашние, индивидуальные задания, подготовка к аудиторным занятиям, контрольным мероприятиям соответствует выделенным долям времени для среднего студента.

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.

Технологическая карта самостоятельной работы студента

Код реализуемой компетенции	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов
1	2	3	4	5
4 / 5 семестр				
ОК-5, ОПК-7	Самостоятельное изучение тем: Тема 1. Концепция информационной безопасности. Защита. Виды противников или нарушителей Тема 2. Анализ способов нарушений информационной безопасности. Тема 3. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Тема 4. Понятия о видах компьютерных вирусов и тренды их развития. Тема 5. Методы криптографии. Тема 6. Основные положения теории информационной безопасности информационных систем. Тема 7. Построение комплексных систем защиты информации. Ис-	Конспект. Выполнение лабораторных работ. Составление справочного материала	Основная и дополнительная литература. Интернет-ресурсы.	67/121

	пользование защищенных компьютерных систем. Тема 8. Модели безопасности и их применение Тема 9. Стандарты информационного обмена и информационная безопасность в санкционных условиях функционирования в России глобальных сетей. Тема 10. Место информационной безопасности экономических систем в Национальной безопасности страны.			
Итого за 4/5 семестр: 67/121				
ИТОГО: 67/121				

При самостоятельном изучении тем используется литература, представленная в разделе 8. Кроме того, студенты могут использовать интернет – ресурсы.

Содержание заданий для самостоятельной работы

Темы для выполнения заданий на самостоятельную работу

1. Традиционные каналы утечки информации.
2. Субъекты и объекты защиты на рынке информационных продуктов и услуг.
3. Информационные ресурсы в негосударственной сфере как объекты обеспечения безопасности.
4. Информационные войны и информационно-программное оружие.
5. Владение информацией как фактор формирования информационной элиты.
6. Историческое развитие понятий информации и информационных ресурсов.
7. Состояние современных информационных факторов угроз личности, общества, государства и субъектам хозяйствования.
8. Методы и способы оценка вероятности наступления угроз.
9. Способы оценки вероятности наступления угроз.
10. Возможные методы давления на пользователей как угрозы для ИС.
11. Индикаторы и измерения для опасностей.
12. Криминальный характер компьютерных преступлений.
13. «Обиженные сотрудники» и исходящие от них потенциальные угрозы.
14. Психологические приемы получения закрытой информации.

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 (тест) для самоконтроля

- 4.5.1. Что понимается под информационным обществом, каковы его характерные черты?
- 4.5.2. Почему информация – это стратегический ресурс?
- 4.5.3. Приведите конкретные примеры охраняемых объектов (по группам).

- 4.5.4. Почему человек считается универсальным носителем и производителем информации?
- 4.5.5. Кто может являться субъектом информационных отношений?
- 4.5.6. Приведите примеры реальных элементов ЗИ в вашем учебном заведении, относящихся к разным направлениям?
- 4.5.7. Почему построение комплекса ЗИ требует системного подхода?
- 4.5.8. Какую информацию можно отнести к защищаемой? Приведите примеры.
- 4.5.9. Что можно сказать о зависимости степени секретности информации и уровня защиты, ее стоимости и круге лиц, допущенных к ней?
- 4.5.10. Кто в нашем государстве обеспечивает сохранность сведений, составляющих государственную или коммерческую тайны?
- 4.5.11. Деятельность каких служб связана с организацией и предотвращением утечек информации?
- 4.5.12. Каковы основные направления разведывательной деятельности иностранных спецслужб, а также конкурентов компании или предприятия в сфере промышленного шпионажа?
- 4.5.13. Попытайтесь сформулировать правила для предотвращения коммерческого шпионажа.
- 4.5.14. Приведите примеры гласных (легальных) методов получения защищаемой информации.
- 4.5.15. Опишите развитие возможных ситуаций с закрытой информацией при ее утечке.
- 4.5.16. Чем отличаются разглашение, раскрытие или распространение? Приведите примеры.
- 4.5.17. Выделите условия, способствующие утечке защищаемой информации. Приведите примеры.
- 4.5.18. Что понимается под абстрактной угрозой?
- 4.5.19. Что характеризует угрозы с точки зрения ИБ ИС?
- 4.5.20. Чем отличаются злоумышленники от нарушителей? Приведите примеры.
- 4.5.21. Какие могут быть уязвимые места в ИС? Приведите примеры.
- 4.5.22. Что понимается под «заплатами», устанавливающимися в защищаемую ИС?
- 4.5.23. Приведите примеры случайных или непреднамеренных угроз и продумайте способы и средства защиты.
- 4.5.24. Приведите примеры преднамеренных угроз и продумайте способы защиты.
- 4.5.25. Наступление каких угроз можно предсказать с определенной вероятностью?
- 4.5.26. Что относится к активам предприятия или организации? Как реализация атаки на активы скажется на ее дальнейшей работе?
- 4.5.27. Перечислите, реализация каких атак повлияет на бизнес.
- 4.5.28. Почему важно применять один подход ко всем активам при решении вопросов реализации ИБ?
- 4.5.29. Почему важно продумать план возврата при анализе наступления угроз ИБ?
- 4.5.30. Дайте характеристики различным методам дублирования информации в ИС.

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 информационной безопасности. Защита. Виды противников или нарушителей.		

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 2. Анализ способов нарушений информационной безопасности.		
Слайд-лекции	Тема 4. Понятия о видах компьютерных вирусов и тренды их развития.		
Слайд-лекции	Тема 4. Методы криптографии.		

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

№	Наименование лабораторных работ	Задание по лабораторным работам
1	Лабораторная работа 1. Источники угроз и уязвимые места информационных систем, виды противников.	Задание. Провести анализ, изучить, определить и расписать источники угроз, уязвимые места информационных систем разных типов, структурировать виды и образы противников или нарушителей в ретроспективе, настоящем периоде и перспективе.
2	Лабораторная работа 2. Компьютерные вирусы.	Задание. Используя различные информационные источники системно и многовариантно характеризовать, описать модели и типы компьютерных вирусов, изучить методы функционирования компьютерных вирусов, а также способы их нейтрализации.
3	Лабораторная работа 3.	Задание. Рассмотреть криптографические методы защиты ин-

№	Наименование лабораторных работ	Задание по лабораторным работам
	Криптография.	формации: основные методы криптографии. Шифрование – симметричные методы и асимметричные методы. Методы защиты целостности данных.
4	Лабораторная работа 4. Стандарты информационной безопасности, построение системы защиты информации.	Задание. Изучить стандарты информационной безопасности в России и ведущих зарубежных странах. Анализировать организацию и построение системы защиты информации, провести сопоставление с анализом особенностей иерархии систем защиты информации инженерно-техническими средствами, кадрово-воспитательными.
5	Лабораторная работа 5. Правовые аспекты информационной защиты.	Задание. Провести анализ, изучить правовые аспекты информационной защиты экономических систем в Российской Федерации. Исследовать правовые аспекты информационной защиты экономических систем на федеральном, региональном и муниципальных уровнях.

Лабораторные работы обеспечивают:

формирование умений и навыков обращения с программным обеспечением, демонстрацию применения теоретических знаний на практике, закрепление и углубление теоретических знаний, контроль знаний и умений в формулировании выводов, развитие интереса к изучаемой дисциплине.

Применение лабораторных работ позволяет вовлечь в активную работу всех обучающихся группы и сформировать интерес к изучению дисциплины.

Самостоятельный поиск ответов на поставленные вопросы и задачи в ходе лабораторной работы приобретают особую значимость в восприятии, понимании содержания дисциплины.

Изученный на лекциях материал лучше усваивается, лабораторные работы демонстрируют практическое их применение.

Лабораторное занятие включает в себя следующие этапы:

- защиту студентами предыдущей лабораторной работы;
- постановка задачи для выполнения лабораторной работы, включая краткие теоретические сведения по рассматриваемому вопросу, обсуждение методики выполнения работы;
- ответы на вопросы студентов;
- подготовка студентами бланков отчетов по выполняемой лабораторной работе;
- осуществление допуска студентов к выполняемой лабораторной работе посредством обсуждения теоретических вопросов по теме занятия;
- непосредственное проведение измерений лабораторной работы;
- подведение итогов занятия.

Для успешного усвоения дисциплины студенты обеспечиваются учебно-методическими материалами по предмету (тематическими планами лекций и лабораторных занятий, необходимой учебной и научной литературой). Во время аудиторных занятий проводится выполнение заданий по заданной тематике, слушание и обсуждение сообщений по самостоятельно изучаемым вопросам, проведение тестирований, ответы на вопросы студентов.

Самостоятельная работа студентов проводится внеаудиторное время и включает в себя изучение литературы и конспектов лекций по дисциплине, выполнение заданий и сообщений по самостоятельно изучаемым вопросам, а также докладов на научно-практическую конференцию.

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
ОК-5 ОПК-7	текущий	устный опрос	4.5.1- 4.5.30
ОК-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: ОК-5 социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. ОПК-7 угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты, обладает способностью определять информационные ресурсы, подлежащие защите.	ОК-5 Развернутый ответ на вопрос с приведением практических примеров: - традиционные каналы утечки информации? Подготовить обзор с использованием Интернет на тему: - информационные войны и информационно-программное оружие? Краткий письменный ответ на вопрос: - почему информация – это стратегический ресурс? ОПК-7 Развернутый ответ на вопрос с приведением практических примеров: - деятельность каких служб связана с организацией и предотвращением утечек информации? Подготовить обзор с использованием Интернет на тему: - правила для предотвращения коммерческого шпионажа? Краткий письменный ответ на вопрос: - субъекты и объекты защиты на рынке информационных продуктов и услуг? Развернутый ответ на вопрос с приведением практических примеров: - владение информацией как фактор формирования информационной элиты? Подготовить обзор с использованием Интернет на тему: - состояние современных информационных факторов угроз личности, общества, государства и субъектам хозяйствования? Краткий письменный ответ на вопрос: - традиционные каналы утечки информации?
Умеет: ОК-5 понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, об-	ОК-5 Развернутый ответ на вопрос с приведением практических примеров: - приведите конкретные примеры охраняемых объектов (по группам)? Подготовить обзор с использованием Интернет на тему: - психологические приемы получения закрытой информации? Краткий письменный ответ на вопрос: - способы оценки вероятности наступления угроз?

Результаты освоения дисциплины	Оценочные средства (перечень вопросов, заданий и др.)
щества и государства, соблюдать нормы профессиональной этики. ОПК-7 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.	ОПК-7 Развернутый ответ на вопрос с приведением практических примеров: - чем отличаются злоумышленники от нарушителей? Подготовить обзор с использованием Интернет на тему: - криминальный характер компьютерных преступлений? Краткий письменный ответ на вопрос: - что понимается под абстрактной угрозой? Развернутый ответ на вопрос с приведением практических примеров: - почему построение комплекса защиты информации требует системного подхода? Подготовить обзор с использованием Интернет на тему: - методы и способы оценки вероятности наступления угроз? Краткий письменный ответ на вопрос: - почему человек считается универсальным носителем и производителем информации?
Имеет практический опыт: ОК-5 в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики, развил способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности ОПК-7 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.	ОК-5 Развернутый ответ на вопрос с приведением практических примеров: - «обиженные» сотрудники и исходящие от них потенциальные угрозы? Подготовить обзор с использованием Интернет на тему: - историческое развитие понятий информации и информационных ресурсов? Краткий письменный ответ на вопрос: - индикаторы и измерения для опасностей? ОПК-7 Развернутый ответ на вопрос с приведением практических примеров: - условия, способствующие утечке защищаемой информации? Подготовить обзор с использованием Интернет на тему: - гласные (легальные) методы получения защищаемой информации? Краткий письменный ответ на вопрос: - преднамеренные угрозы и способы защиты? Развернутый ответ на вопрос с приведением практических примеров: - случайные или непреднамеренные угрозы, средства и способы защиты? Подготовить обзор с использованием Интернет на тему: - перечислите, реализация каких атак повлияет на бизнес? Краткий письменный ответ на вопрос: - развитие возможных ситуаций с закрытой информацией при ее утечке на предприятие?

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 оце-

но 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 балльная шкала, %	100 балльная 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. 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>

5. 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

6. 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.
7. Бабаш, А. В. Информационная безопасность. Лабораторный практикум [Текст] : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - М. : КноРус, 2012. - 131 с.
8. Белоножкин, В. И. Информационные аспекты противодействия терроризму [Текст] / В. И. Белоножкин, Г. А. Остапенко. - М. : Горячая линия - Телеком, 2009. - 112 с.
9. Введение в информационную безопасность [Текст] : учеб. пособие для вузов / А. А. Малиук [и др.] под ред. В. С. Горбатова. - М. : Горячая линия - Телеком, 2011. - 288 с.
10. Гашков, С. Б. Криптографические методы защиты информации [Текст] : учеб. пособие для вузов по направлениям "Приклад. математика и информатика" и "Информ. технологии" / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - М. : Академия, 2010. - 298 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. Петраков под 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 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	EPWin	Средство моделирования	Построение моделей
6	Secret Net	Система защиты информации	Средство защиты информации от несанкционированного доступа
7	vipNet (client, coordinator, administrator)	Система защиты информации	Средство защиты информации
8	Антивирус Касперского	Система защиты информации	Средство защиты информации и оборудования
9	КриптоПро	Система защиты информации	Средство защиты информации
10	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 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 информационной безопасности»

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

[illegible]

