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 «Программно-аппаратные средства защиты информации»
для студентов направления подготовки 10.03.01 «Информационная безопасность»
направленности «Организация и технология защиты информации»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине «Программно-аппаратные средства защиты информации» включена в основную профессиональную образовательную программу направленности (профиля) «Организация и технология защиты информации» направления подготовки 10.03.01 «Информационная безопасность» 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 «Программно-аппаратные средства защиты информации» разработана в соответствии с Федеральным государственным образовательным стандартом направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Минобрнауки России от 01.12.2016 г. № 1515.

Составили: Козлов Д.В., Любивая Т.Г.

Согласовано Директор научной библиотеки _____ В.Н. Еремина

Согласовано Начальник управления информатизации _____ В.В. Обухов

Рабочая программа утверждена на заседании кафедры «Прикладная информатика в экономике»
Протокол № 12 от 22.06.2018 г.

Заведующий кафедрой _____ д.э.н., профессор 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

Целями освоения дисциплины являются:

– изучение программных, программно-аппаратных и технических средств защиты информации;

– формирование умений и навыков установки, настройки, эксплуатации и поддержания в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований.

1.2. В соответствии с видами профессиональной деятельности, на которые ориентирована образовательная программа указанного направления подготовки, содержание дисциплины позволит обучающимся решать следующие профессиональные задачи:

эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем.

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины у обучающихся формируются следующие компетенции:

Код компетенции	Наименование компетенции
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.
ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

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*:** принципы организации информационных систем в соответствии с требованиями по защите информации (ОПК-7); процедуры организации и проведения контрольных проверок работоспособности и эффективности программных, программно-аппаратных и технических средств защиты	Лекции	Устный опрос

информации (ПК-6).		
Умеет: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах (ОПК-7); анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах (ОПК-7); выполнять проверку работоспособности и эффективности программных, программно-аппаратных и технических средств защиты информации (ПК-6).	Лабораторные работы	Защита отчётов по лабораторным работам
***Имеет практический опыт*:** проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы (ОПК-7); участия в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6).	Лабораторные работы	Защита отчётов по лабораторным работам

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части.

Её освоение осуществляется в 7 семестре.

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код компетенции(й)
	Предшествующие дисциплины	
1.	Аппаратные средства вычислительной техники	ПК-1, ПК-6
2.	Техническая защита информации	ОПК-7, ПСК-1, ПК-15
	Последующие дисциплины	
1.	Защита информационных процессов в компьютерных	ОПК-7

	системах и телекоммуникационных сетях	
2.	Организация и управление службой ЗИ	ПК-5, ПК-7, ПК-13, ПК-14, ПК-15

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	144 ч. 4 з.е.	144 ч. 4 з.е.	-
Лекции (час)	22 ч.	6 ч.	-
Практические занятия (час)	-	-	-
Лабораторные работы (час)	32 ч.	8 ч.	-
Самостоятельная работа (час)	63 ч.	121 ч.	-
Курсовой проект (+,-)	+	+	-
Контрольная работа (+,-)	-	-	-
Экзамен, семестр/час	7 семестр/27 ч.	7 семестр/9 ч.	-
Зачет (дифференцированный зачет), семестр	-	-	-
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. Задачи программно-аппаратной защиты информации.	4/1/-	-/-/-	8/2/-	9/17/-	Устный опрос, защита лабораторных работ
2.	Тема 2. Защита файлов от изменения; электронная цифровая подпись (ЭЦП).	4/1/-	-/-/-	-/-/-	9/17/-	Устный опрос
3.	Тема 3. Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных.	4/1/-	-/-/-	8/2/-	9/17/-	Устный опрос, защита лабораторных работ
4.	Тема 4. Защита алгоритма шифрования; принцип	2/0,5/-	-/-/-	-/-/-	9/17/-	Устный опрос

	чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты.					
5.	Тема 5. Методы и средства ограничения доступа к компонентам ЭВМ.	2/0,5/-	-/-/-	8/2/-	9/17/-	Устный опрос, защита лабораторных работ
6.	Тема 6. Защиты программ от несанкционированного копирования.	4/1/-	-/-/-	-/-/-	9/17/-	Устный опрос
7.	Тема 7. Компьютерные вирусы как особый класс разрушающих программных воздействий (РПВ); необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.	2/1/-	-/-/-	8/2/-	9/19/-	Устный опрос, защита лабораторных работ
	Промежуточная аттестация по дисциплине	22/6/-	-/-/-	32/8/-	63/121/-	Курсовой проект, экзамен

Примечание:
-/-/-, объем часов соответственно для очной, очно-заочной, заочной форм обучения.

4.2.Содержание практических занятий

Практические занятия учебным планом не предусмотрены.

4.3. Содержание лабораторных работ

№	Наименование лабораторных работ	Обьем часов	Наименование темы дисциплины
1.	Лабораторная работа 1. «Основы безопасности операционной системы Windows»	8/2/-	Введение. Задачи программно-аппаратной защиты информации.
2.	Лабораторная работа 2. «Прикладная криптосистема PGP Freeware»	8/2/-	Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных
3.	Лабораторная работа 3. «Сканер безопасности XSpider»	2/0,5/-	Методы и средства ограничения доступа к компонентам ЭВМ
4.	Лабораторная работа 4. «Персональный межсетевой экран Outpost Firewall Free»	2/0,5/-	Методы и средства ограничения доступа к компонентам ЭВМ
5.	Лабораторная работа 5. «Сетевой сниффер»	4/1/-	Методы и средства ограничения доступа к компонентам ЭВМ
6.	Лабораторная работа 6. «Антивирусный пакет Kaspersky Endpoint Security»	8/2/-	Компьютерные вирусы как особый класс РПВ; необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды
	Итого	32/8/-	

Примечание:

-/-/-, объем часов соответственно для очной, очно-заочной, заочной форм обучения.

5. 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
ОПК-7, ПК-6	Работа с литературой, подготовка доклада на конференцию	Конспект, доклад	Собеседование, опубликование тезисов доклада	63/121/-
			Итого	63/121/-

Рекомендуемая литература: 1, 2, 3, 4, 5, 6.

Содержание заданий для самостоятельной работы

Вопросы для самоконтроля

1. Предмет и задачи программно-аппаратной защиты информации.
2. Архитектура системы программно-аппаратной защиты.
3. Идентификация субъекта. Понятия идентификации и аутентификации.
4. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.
5. Простая аутентификация.
6. Аутентификация на основе многоразовых паролей.
7. Аутентификация на основе одноразовых паролей. Аутентификация на основе сертификатов.
8. Биометрическая идентификация и аутентификация пользователей.
9. Строгая аутентификация.
10. Протоколы аутентификации с симметричными алгоритмами шифрования.
11. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций.
12. Аутентификация с использованием асимметричных алгоритмов шифрования.
13. Аутентификация, основанная на использовании цифровой подписи.
14. Протоколы аутентификации с нулевой передачей значений.
15. Механизм идентификации и аутентификации в ОС Windows.
16. Протокол идентификации и аутентификации в ОС Windows.
17. Основные подходы к защите данных от несанкционированного доступа (НСД).
18. Модели типовых политик безопасности компьютерных средств защиты информации.
19. Основные подходы к защите данных от НСД: шифрование.
20. Основные подходы к защите данных от НСД: контроль доступа и разграничение доступа.
21. Основные подходы к защите данных от НСД: иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам.
22. Доступ к данным со стороны процесса.
23. Основные подходы к защите данных от НСД: надежность систем ограничения доступа.
24. Основные подходы к защите данных от НСД: защита файлов от изменения.
25. Электронная цифровая подпись (ЭЦП): алгоритм действия ЭЦП.

26. Электронная цифровая подпись (ЭЦП): удостоверяющие центры и их функции.
27. Электронная цифровая подпись (ЭЦП): основные варианты программной реализации алгоритмов ЭЦП.
28. Программно-аппаратные средства шифрования.
29. Построение аппаратных компонент криптозащиты данных.
30. Защита алгоритма шифрования.
31. Принцип чувствительной области и принцип главного ключа.
32. Необходимые и достаточные функции аппаратного средства криптозащиты.
33. Методы и средства ограничения доступа к компонентам ЭВМ.
34. Методы и средства защиты программ от несанкционированного копирования.
35. Пароли и ключи, организация хранения ключей.
36. Защита программ от изучения, отладки, дизассемблирования, трассировки по прерываниям.
37. Классификация и виды разрушающих программных воздействий (РПВ).
38. Защита от разрушающих программных воздействий (РПВ).
39. Классификация вирусов.
40. Механизмы заражения компьютерными вирусами.
41. Методы и средства защиты от компьютерных вирусов.
42. Профилактика заражения вирусами компьютерных систем.
43. Структура антивирусной защиты предприятия.
44. Необходимые и достаточные условия недопущения разрушающего воздействия.
45. Понятие изолированной программной среды.

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-лекция	Тема 2. Защита файлов от изменения; электронная цифровая подпись (ЭЦП).		

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 компетенций и оценка текущей успеваемости по дисциплине. По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации. Списки учебных пособий, научных трудов, которые студентам следует прочесть и законспектировать, темы лабораторных работ, вопросы к экзамену 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 изучается студентами самостоятельно. Самостоятельная работа предусматривает подготовку к аудиторным занятиям, выполнение заданий, подготовку к промежуточной аттестации.

На лекционных и практических 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 (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

№	Наименование лабораторных работ	Задание по лабораторным работам
1.	Лабораторная работа 1. «Основы безопасности операционной системы Windows»	Задания по лабораторной работе представлены в учебно-методическом комплексе [2] с. 59-102.
2.	Лабораторная работа 2. «Прикладная криптосистема PGP Freeware»	Задания по лабораторной работе представлены в учебно-методическом комплексе [2] с. 102-125.
3.	Лабораторная работа 3. «Сканер безопасности XSpider»	Задания по лабораторной работе представлены в учебно-методическом комплексе [2] с. 125-138.
4.	Лабораторная работа 4. «Персональный межсетевой экран Outpost Firewall Free»	1. Установить и настроить Outpost Firewall Free. 2. Изучить функционирование модуля «Быстрая настройка».
5.	Лабораторная работа 5. «Сетевой сниффер»	Задания по лабораторной работе представлены в учебно-методическом комплексе [2] с. 151-162.
6.	Лабораторная работа 6. «Антивирусный пакет Kaspersky Endpoint Security»	1. Установить и настроить Kaspersky Endpoint Security. 2. Выполнить антивирусное сканирование локального диска С: 3. Настроить отправку уведомлений об обнаружении вирусов на домашний e-mail.

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.

6.2. Методические указания для выполнения контрольных работ

Контрольная работа по дисциплине учебным планом не предусмотрена.

6.3. Методические указания для выполнения курсового проекта

Курсовой проект по дисциплине «Программно-аппаратные средства защиты информации» по правилам оформления должен соответствовать требованиям к курсовым проектам, утвержденным на кафедре.

Курсовой проект позволяет закрепить и углубить знания по дисциплине «Программно-аппаратные средства защиты информации», приобрести навыки использования современных научных достижений в разработке программных и аппаратных средств защиты информации и является подтверждением того, что студент умеет применять полученные знания при решении конкретной задачи.

Целью выполнения курсового проекта является приобретение студентами практических навыков в построения систем защиты информации, изучении структуры, основного назначения и характерных особенностей программного и аппаратного обеспечения защиты и безопасности информации в компьютерных системах.

В задачи курсового проекта по дисциплине «Программно-аппаратные средства защиты информации» входит:

– получение знаний в области программного и аппаратного обеспечения защиты и безопасности информации;
– изучение средств и методов защиты информации;
– развитие системного мышления;
– умение обобщать информацию и делать соответствующие выводы.

Последовательность выполнения курсового проекта:

– провести теоретическое исследование;
– составить и утвердить техническое задание;
– на основе знаний, полученных в результате исследования и лекционных занятий, разработать программу по защите информации;
– составить отчёт по работе с описанием всех пунктов задания.

Структура проекта включает:

1. Введение: обзор состояния вопроса, характеристика объекта исследования.

2. Аналитическая часть:

1) Описание предметной области: структура предприятия, основные виды деятельности и процессы, основные объекты инфраструктуры.

2) Структура информационной системы предприятия.

3) Задачи обеспечения ИБ на предприятии и задачи программно-аппаратной защиты информации на предприятии.

4) Анализ и выявление объектов защиты.

5) Анализ и выявление возможных каналов утечки информации и несанкционированного доступа к ресурсам, основных угроз.

6) Техническое задание на разработку системы, предложения по повышению уровня защиты (по согласованию с руководителем).

2. Проектная часть:

1) Определение каналов утечки информации и несанкционированного доступа к ресурсам с привязкой к объектам.

2) Анализ и выбор основных подходов к программно-аппаратной защите информации на предприятии.

3) Определение основных элементов системы ПЗИ предприятия.

4) Планирование защитных мероприятий по различным направлениям (по объектам, по видам угроз, по видам дестабилизирующего воздействия).

5) Разработка системы (программного модуля), предложения по повышению уровня защиты.

Общий объем курсового проекта – не менее 40 страниц.

Примерная тематика курсовых проектов

1. Разработка системы программно-аппаратной защиты информации предприятия.
2. Совершенствование системы программно-аппаратной защиты информации предприятия.
3. Разработка методов программно-аппаратной защиты источников информации.
4. Разработка модели угроз безопасности информации, защищаемой техническими средствами.
5. Программно-аппаратные средства шифрования.
6. Средства аудита систем информационной безопасности.
7. Средства мониторинга информационных систем.
8. Средства мониторинга локальных сетей.
9. Системы обнаружения атак и вторжений.
10. Средства антивирусной защиты информационных систем.
11. Межсетевые экраны и их применение при защите информации.
12. Виртуальные сети и их применение при защите информации.
13. Программные средства работы с электронной цифровой подписью.
14. Реализация криптографических методов защиты информации в Windows.
15. Методы идентификации субъекта.
16. Контроль доступа и разграничение доступа.
17. Защита файлов от изменения.
18. Программно-аппаратные средства шифрования.
19. Построение аппаратных компонент криптозащиты данных.
20. Методы и средства ограничения доступа к компонентам ЭВМ.
21. Защита программ от несанкционированного копирования.
22. Защита программ от разрушающих программных воздействий.
23. Компьютерные вирусы как особый класс разрушающих программных воздействий.

7. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Фонды оценочных средств, позволяющие оценить уровень сформированности компетенций и результаты освоения дисциплины, представлены следующими компонентами:

Код оцениваемой компетенции (или её части)	Тип контроля	Вид контроля	Количество элементов, шт.
ОПК-7, ПК-6	текущий	устный опрос	45
ОПК-7, ПК-6	текущий	защита отчётов по лабораторным работам	6
ОПК-7, ПК-6	промежуточный	вопросы типа «Эссе»	30

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

Результаты освоения дисциплины	Оценочные средства
***Знает*:** принципы организации информационных систем в соответствии с требованиями по защите информации (ОПК-7); процедуры организации и проведения контрольных проверок работоспособности	Ответить на вопросы: 1. Архитектура системы программно-аппаратной защиты. 2. Идентификация субъекта. Понятия идентификации и аутентификации. 3. Механизм идентификации и

и эффективности программных, программно-аппаратных и технических средств защиты информации (ПК-6).	аутентификации в ОС Windows. 4. Основные подходы к защите данных от несанкционированного доступа (НСД). 5. Модели типовых политик безопасности компьютерных средств защиты информации. 6. Электронная цифровая подпись (ЭЦП): алгоритм действия ЭЦП. 7. Программно-аппаратные средства шифрования. 8. Методы и средства ограничения доступа к компонентам ЭВМ. 9. Защита от разрушающих программных воздействий (РПВ). 10. Механизмы заражения компьютерными вирусами.
Умеет: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах (ОПК-7); анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах (ОПК-7); выполнять проверку работоспособности и эффективности программных, программно-аппаратных и технических средств защиты информации (ПК-6).	Лабораторная работа 1. «Основы безопасности операционной системы Windows». Лабораторная работа 2. «Прикладная криптосистема PGP Freeware». Лабораторная работа 3. «Сканер безопасности XSpider». Лабораторная работа 4. «Персональный межсетевой экран Outpost Firewall Free». Лабораторная работа 5. «Сетевой снифер». Лабораторная работа 6. «Антивирусный пакет Kaspersky Endpoint Security».
***Имеет практический опыт*:** проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы (ОПК-7); участия в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6).	Лабораторная работа 1. «Основы безопасности операционной системы Windows». Лабораторная работа 2. «Прикладная криптосистема PGP Freeware». Лабораторная работа 3. «Сканер безопасности XSpider». Лабораторная работа 4. «Персональный межсетевой экран Outpost Firewall Free». Лабораторная работа 5. «Сетевой снифер». Лабораторная работа 6. «Антивирусный пакет Kaspersky Endpoint Security».

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-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. Защита информации [Электронный ресурс] : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук [и др.]. - 2-е изд. - Документ HTML. - М. : РИОР [и др.], 2015. - 393 с. - Режим доступа: http://znanium.com/bookread.php?book=474838.

2. Учебно-методический комплекс по дисциплине "Программно-аппаратные средства защиты информации" [Электронный ресурс] : для студентов направления подгот. 10.03.01 "Информ. безопасность" / Поволж. гос. ун-т сервиса (ПВГУС), Каф. "Приклад. информатика в экономике" ; сост.: С. М. Бобровский. - Документ Adobe Acrobat. - Тольятти : ПВГУС, 2016. - 5,99 МБ, 196 с. - Режим доступа: http://elib.tolgas.ru.

3. Хорев, П. Б. Программно-аппаратная защита информации [Электронный ресурс] : учеб. пособие для вузов по направлению "Информ. безопасность" / П. Б. Хорев. - 2-е изд., испр. и доп. - Документ Bookread2. - М. : ФОРУМ, 2015. - 351 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=489084.

4. 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

5. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Документ Reader. - СПб. [и др.] : Лань, 2018. - 92 с. - Режим доступа: https://e.lanbook.com/reader/book/107306/#1.

6. Яшин, В. Н. Информатика. Программные средства персонального компьютера [Электронный ресурс] : учеб. пособие для вузов по направлению "Приклад. информатика" и др. экон. специальностям / В. Н. Яшин. - Документ Bookread2. - М. : ИНФРА-М, 2018. - 236 с. - Режим доступа: http://znanium.com/bookread2.php?book=937489.

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

Интернет-ресурсы

1. ИНТУИТ. Национальный открытый университет [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/. – Загл. с экрана.
2. Российское образование [Электронный ресурс] : федер. портал. - Режим доступа: http://www.edu.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 доступа: http://znanium.com/. - Загл. с экрана.

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

Краткая характеристика применяемого программного обеспечения

№ п/п	Программный продукт	Характеристика	Назначение при освоении дисциплины
1.	Microsoft Office	Пакет прикладных программ	Оформление отчетов по лабораторным работам
2.	PGP Freeware	Прикладная криптосистема	Выполнение лабораторных работ
3.	XSpider	Сканер безопасности	Выполнение лабораторных работ
4.	Outpost Firewall Free	Персональный межсетевой экран	Выполнение лабораторных работ
5.	Kaspersky Endpoint Security	Антивирусный пакет	Выполнение лабораторных работ

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 «Комплексная лаборатория программно-аппаратных средств обеспечения информационной безопасности, сетей и систем передачи информации», 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 «Программно-аппаратные средства защиты информации»

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

№	Виды контрольных точек	Количество контрольных точек	Количество баллов за 1 контрольную точку	Срок прохождения контрольных точек																		Итого	Зачетно-экзаменационная сессия
				Сентябрь				Октябрь					Ноябрь				Декабрь						
1.	Обязательные задания:																						
1.1.	Выполнение лабораторных работ	7	10		+		+		+		+		+		+		+					70	
2.	Дополнительные задания																						
2.1.	Итоговый контроль	1	30															+				30	
	Общий рейтинг по дисциплине:																					100	
	Форма контроля																						Экзамен