Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков

« 21 » сентября 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Методы и средства защиты программного обеспечения
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: бакалавриат
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 144 (4)
(часы (ЗЕ))

Направление подготовки: 10.03.01 Информационная безопасность
(код и наименование направления)

Направленность: Информационная безопасность (общий профиль, СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

формирование компетентности в области разработки и эксплуатации автоматизированных систем в защищенном исполнении, отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документации по обес-печению безопасности информации.

1.2. Изучаемые объекты дисциплины

изучение основных угроз безопасности информации в автоматизированных системах и освоение методик оценки данных угроз; формирование умений использования методов, способов и средств разработки автоматизированных систем и подсистем безопасности автоматизированных систем; изучение основных мер по защите информации в автоматизированных системах; овладение навыками управления деятельностью персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-2.1	ИД-1ПК-2.1	Знает принципы организации и структуру систем защиты информации современных операционных систем; критерии оценки эффективности и надежности систем защиты информации операционных систем; основные протоколы, используемые для защиты информации в вычислительных сетях; основные криптографические методы, используемые для защиты информации в вычислительных сетях; Знает принципы построения и функционирования локальных и глобальных вычислительных сетей; последовательность и содержание этапов построения локальных вычислительных сетей; принципы построения и функционирования, примеры реализаций современных операционных систем; принципы построения и функционирования, примеры реализаций современных систем управления базами данных	Знает национальные, межгосударственные и международные стандарты в области защиты информации; нормативные правовые акты в области защиты информации; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем; руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации.	Зачет
ПК-2.1	ИД-2ПК-2.1	Умеет конфигурировать параметры системы защиты информации современных операционных систем; контролировать эффективность принятых мер по реализации политик безопасности информации в современных	Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на	Отчёт по практическому занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		операционных системах; проводить анализ угроз безопасности в локальных вычислительных сетях;Умеет использовать средства защиты информации операционных систем; разрабатывать и администрировать базы данных	соответствие требованиям по безопасности информации и техническим условиям.	
ПК-2.1	ИД-3ПК-2.1	Владение навыками - Централизованной настройки информационной безопасности Windows Active Directory и интеграции АИС в AD; Понимание методов программной защиты информации. - Управления правами пользователей. Локальная и групповая политики безопасности в Windows и Linux; - Организации многорубежной системы охраны;	Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы; разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НДС и специальных воздействий на соответствие техническим условиям	Индивидуальное задание

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	63	63
- лекции (Л)	22	22
- лабораторные работы (ЛР)	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	22	22
- контроль самостоятельной работы (КСР)	3	3
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	81	81
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	144	144

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
8-й семестр				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Безопасность информационных систем	6	0	6	30
Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Международные стандарты информационного обмена. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet Виды угроз информационной безопасности. Три вида возможных нарушений информацион-ной системы. Защита. Источники угроз информационной безопасности РФ. Информа-ционная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Удаленные атаки на интрасети Стандарты безопасности. Критерии безопасности компьютерных систем «Оранжевая книга». Руководящие документы Гостехкомиссии				
Методы обеспечения безопасности информационных систем	8	8	6	30
Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Международные стандарты информационного обмена. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet Виды угроз информационной безопасности. Три вида возможных нарушений информацион-ной системы. Защита. Источники угроз информационной безопасности РФ. Информа-ционная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Удаленные атаки на интрасети Стандарты безопасности. Критерии безопасности компьютерных систем «Оранжевая книга». Руководящие документы Гостехкомиссии				
Программные методы обеспечение информационной безопасности	8	8	10	21
Архитектура операционных систем. Процесс загрузки операционных систем. Классификиция программного обеспечения. Защищенный режим работы процессора. Уровни доступа. Разграничение адресного пространства и ресурсов ПК. Драйверы. Сервисы. Утилиты				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Методы криптографии. Классификация криптографических методов. Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись. Программные интерфейсы Crypto API Условия существования вредоносных программ. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы. Rootkit. Спам. Защита от компьютерных вирусов. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы Виды угроз. Разграничение доступа к ресурсам ИС. Идентификация и аутентификация пользователей в ОС семейства Windows и Linux. Аудит событий безопасности. Администрирование прав пользователей. Аппаратно-программные комплексы обеспечения безопасности ОС Управление доступом к ресурсам в программном коде. Получение информации об иденти-фикации и аутентификации пользователей в ОС семейства Windows и Linux. Использование встроенных API шифрования Crypto API. Исследование программного кода для работы с электронными ключами				
ИТОГО по 8-му семестру	22	16	22	81
ИТОГО по дисциплине	22	16	22	81

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Модель угроз. Модель нарушителя. Классы информационных систем
2	Понятие и сущность программной защиты информации. Управление правами пользователей. Локальная политика безопасности в Windows и Linux
3	Вирусы. Руткиты. Антивирусы. Архитектура и возможности про-граммного обеспечения антивирусов. Интеграция в файловую и сетевую подсистемы.
4	Электронные ключи и смарт-карты для обеспечения разграниче-ния доступа и шифрования.
5	Программные интерфейсы и библиотеки криптопровайдеров Crypto API.
6	Разработка защищенного клиент-серверного программного обеспечения для заданной предметной области

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Локальная безопасность Windows и анализ уязвимостей операци-онной системы
2	Использование программного обеспечения шифрования данных. Использование безопасных протоколов передачи данных. Перехват трафика с использованием ПО Wireshark
3	Централизованная настройка информационной безопасности Win-dows Active Directory и интеграция Samba Server в AD
4	Настройка типового антивируса. Обновление баз. Настройка фай-ервола. Поиск вирусной активности с использованием реестра, диспетчера процессов, файловых менеджеров
5	Настройка виртуальной машины Virtual PC. Поиск уязвимостей сканерами безопасности. Настройка локальной политики безопас-ности и аудита. Установка прав на доступ к файловым объектам, реестру и журналам событий. Использование Kali Linux для реали-зации атак и закрытие уязвимостей

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	От хранения данных к управлению информацией : учебник для вузов пер. с англ. / . 2-е изд Санкт-Петербург [и др.] : Питер, 2016. 543 с. 43,86 усл. печ. л.	11
2	Шаньгин В. Ф. Информационная безопасность и защита информации. Москва : ДМК Пресс, 2017. 702 с. 43,875 усл. печ. л.	3
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Бабаш А. В., Баранова Е. К., Мельников Ю. Н. Информационная безопасность. Лабораторный практикум : учебное пособие для вузов. Москва : КНОРУС, 2012. 131 с. 8,5 усл. печ. л.	2
2	Т.Кайт. Oracle для профессионалов / Том Кайт Кн.2: Расширение возмож-ностей и защита .— 2-е изд. — 2004 .— 831 с	3
3	Т.Кайт. Oracle для профессионалов : пер. с англ. / Том Кайт. Кн. 1: Архи-тектура и основные особенности .— 2-е изд. — 2004 .— 662 с	3
4	Хорев П. Б. Программно-аппаратная защита информации : учебное пособие. 3-е изд., испр. и доп Москва : ИНФРА-М, 2020. 326 с. 20,44 усл. печ. л.	5
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Основы языка PL/SQL	https://cloud.mail.ru/public/rKNf/RbkbaaefR	сеть Интернет; свободный доступ
Дополнительная литература	Основы языка SQL	https://cloud.mail.ru/public/rKNf/RbkbaaefR	сеть Интернет; свободный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Прикладное программное обеспечение общего назначения	Oracle VM VirtualBox (GNU GPL 2)
Среды разработки, тестирования и отладки	PostgreSQL (PostgreSQL License)

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лабораторная работа	Персональный компьютер	12

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	проектор	1
Практическое занятие	Персональный компьютер	12

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине «Методы и средства защиты программного обеспечения»
Приложение к рабочей программе дисциплины

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль) образовательной программы: Организация и технологии защиты информации

Квалификация выпускника: Бакалавр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 4 **Семестр**: 8

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч.

Форма промежуточной аттестации:
Диф.Зачет: 8 семестр

Пермь 2023

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (8-го семестра учебного плана) и разбито на 2 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по практическим занятиям и диф.зачета. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ОЛР/ ОПЗ**	**Т/КР**		**Зачёт**
Усвоенные знания						
З.1 Знает архитектуру подсистем защиты информации в операционных системах; виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению; источники угроз информационной безопасности программного обеспечения и меры по их предотвращению		ТО1	ОПЗ1 ОПЗ2	КР1		ТВ
Освоенные умения						
У.1 Умеет обосновывать правила безопасной эксплуатации программного обеспечения; осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения.			ОПЗ3 ОЛР1 ОЛР2 ОЛР3	КР2		ПЗ
Приобретенные владения						
В.1 Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования			ОПЗ4 ОПЗ5 ОПЗ6 ОЛР4 ОЛР5			

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОПЗ – отчет по практическому занятию; Т/КР – рубежное тестирование (контрольная работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание дифференцированного зачета.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде диф.зачета, проводимая с учётом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по практическому занятию, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме

защиты отчетов по практическому занятию и рубежных контрольных работ (после проведения практических занятий).

2.2.1. Защита отчетов по практическому занятию

Всего запланировано 6 практических занятий (ПЗ).

Типовые темы ПЗ:

1 Модель угроз. Модель нарушителя. Классы информационных систем

2 Понятие и сущность программной защиты информации. Управление правами пользователей. Локальная политика безопасности в Windows и Linux

3 Вирусы. Руткиты. Антивирусы. Архитектура и возможности программного обеспечения антивирусов. Интеграция в файловую и сетевую подсистемы.

4 Электронные ключи и смарт-карты для обеспечения разграничения доступа и шифрования.

5 Программные интерфейсы и библиотеки криптопровайдеров Crypto API.

6 Разработка защищенного клиент-серверного программного обеспечения для заданной предметной области.

Защита отчетов по практическому занятию проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.2.1. Защита отчетов по Лабораторным работам

Всего запланировано 5 лабораторных работ (ЛР).

Типовые темы ЛР:

1 Локальная безопасность Windows и анализ уязвимостей операционной системы

2 Использование программного обеспечения шифрования данных. Использование безопасных протоколов передачи данных. Перехват трафика с использованием ПО Wireshark

3 Централизованная настройка информационной безопасности Windows Active Directory и интеграция Samba Server в AD

4 Настройка типового антивируса. Обновление баз. Настройка файервола. Поиск вирусной активности с использованием реестра, диспетчера процессов, файловых менеджеров

5 Настройка виртуальной машины Virtual PC. Поиск уязвимостей сканерами безопасности. Настройка локальной политики безопасности и аудита. Установка прав на доступ к файловым объектам, реестру и журналам событий. Использование Kali Linux для реализации атак и закрытие уязвимостей

Защита отчетов по ЛР проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.2.3. Рубежная контрольная работа

Всего запланировано 2 рубежные контрольные работы (КР) после освоения студентами учебных модулей дисциплины и проведения практических занятий.

Типовые задания КР1:

1. Классификация информационной системы и обоснование требований ИБ.
2. Разработка модели угроз и модели нарушителя.
3. Обнаружение уязвимостей и разработка мер по их устранению.

Типовые задания КР2:

1. Выбор программно-аппаратных СЗИ и их конфигурации для защиты сетевой АИС.

2. Анализ сетевой активности, исследование сетевых пакетов

3. Локальные политики безопасности ОС

4. Групповые политики безопасности ОС

Типовые шкала и критерии оценки результатов рубежной контрольной работы приведены в общей части ФОС образовательной программы.

2.3. Выполнение комплексного индивидуального задания на самостоятельную работу

Не предусмотрено.

2.4. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех отчетов по практическим занятиям и положительная интегральная оценка по результатам текущего и рубежного контроля.

2.4.1. Процедура промежуточной аттестации без дополнительного аттестационного испытания

Промежуточная аттестация проводится в форме диф.зачета. Диф.зачет по дисциплине основывается на результатах выполнения предыдущих индивидуальных заданий студента по данной дисциплине.

Критерии выведения итоговой оценки за компоненты компетенций при проведении промежуточной аттестации в виде диф.зачета приведены в общей части ФОС образовательной программы.

2.4.2. Процедура промежуточной аттестации с проведением аттестационного испытания

В отдельных случаях (например, в случае переаттестации дисциплины) промежуточная аттестация в виде диф.зачета по дисциплине может проводиться с проведением аттестационного испытания по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций.

2.4.2.1. Типовые вопросы и задания для диф.зачета по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1 Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Международные стандарты информационного обмена.

2 Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet

3 Виды угроз информационной безопасности. Три вида возможных нарушений информацион-ной системы.

4 Защита. Источники угроз информационной безопасности РФ. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».

5 Удаленные атаки на интрасети

6 Стандарты безопасности. Критерии безопасности компьютерных систем «Оранжевая книга». Руководящие документы Гостехкомиссии

7 Архитектура операционных систем. Процесс загрузки операционных систем. Классификиция программного обеспечения. Защищенный режим работы процессора. Уровни доступа. Разграничение адресного пространства и ресурсов ПК. Драйверы. Сервисы. Утилиты

8 Методы криптографии. Классификация криптографических методов. Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись. Программные интерфейсы Crypto API

9 Условия существования вредоносных программ. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы. Rootkit. Спам. Защита от компьютерных вирусов. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы

10 Виды угроз. Разграничение доступа к ресурсам ИС. Идентификация и аутентификация пользователей в ОС семейства Windows и Linux. Аудит событий безопасности. Администрирование прав пользователей. Аппаратно-программные комплексы обеспечения безопасности ОС

11 Управление доступом к ресурсам в программном коде. Получение информации об иденти-фикации и аутентификации пользователей в ОС семейства Windows и Linux. Использование встроенных API шифрования Crypto API. Исследование программного кода для работы с электронными ключами

Типовые вопросы и практические задания для контроля освоенных умений:

1. Решение ситуационных задач по исследованию объекта, выбору и применению СЗИ на заданном объекте.

2.4.2.2. Шкалы оценивания результатов обучения на диф.зачете

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания.

Типовые шкала и критерии оценки результатов обучения при сдаче диф.зачета для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при диф.зачете считается, что *полученная оценка за компонент*

проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины.

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде диф.зачета используются типовые критерии, приведенные в общей части ФОС образовательной программы.