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

« 18 » июля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Программно-аппаратные средства защиты информации
(наименование)

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

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

Общая трудоёмкость: 108 (3)
(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 компетенций в области разработки и эксплуатации программно-аппаратных средств, используемых для обеспечения информационной безопасности автоматизированных систем

1.2. Изучаемые объекты дисциплины

виды и классификация программных и аппаратных средства защиты автоматизированных систем; модели данных, систем и процессов защиты информации; угрозы безопасности информации в автоматизированных системах; схемы аутентификации в автоматизированных системах, использующие программные и аппаратные средства; методы и модели генерации и управления ключами; методы интеграции программных и аппаратных средства защиты в информационные системы; методы и средства обнаружения и предотвращения вторжений; средства антивирусной защиты в автоматизированных системах; методы построения виртуальных сетей в автоматизированных системах; методы, способы и средства обеспечения отказоустойчивости программных и аппаратных комплексов

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
ОПК-9	ИД-1ОПК-9	Знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем	Знает принципы построения систем и сетей электросвязи; современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем; основные понятия и задачи криптографии, математические модели криптографических систем; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы; национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения; классификацию и количественные характеристики технических каналов утечки информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;	Зачет
ОПК-9	ИД-2ОПК-9	Умеет анализировать программные и программно-аппаратные решения при проектировании систем	Умеет проводить анализ показателей эффективности сетей и систем телекоммуникаций и качества	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
		защиты информации с целью выявления уязвимостей. развертывать и настраивать программные и аппаратные средства для защиты локальных и распределенных вычислительных систем;	предоставляемых услуг; применять математические модели для оценки стойкости СКЗИ; использовать СКЗИ в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации; анализировать и оценивать угрозы информационной безопасности объекта информатизации;	
ОПК-9	ИД-3ОПК-9	Владеет навыками анализа уязвимости программных и программно-аппаратных средств системы защиты информации	Владеет методами и средствами технической защиты информации	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	24	24
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	28	28
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	54	54
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет		
Зачет	9	9
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	108	108

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
7-й семестр				
Безопасность локальных вычислительных систем	8	0	8	20
Предмет и задачи программно-аппаратной защиты информации. Автоматизированная система (АС). Структура и компоненты АС. Сети ЭВМ. Электронный документ (ЭД). Виды информации в КС. Информационные потоки в КС. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Несанкционированное копирование программ как особый вид НСД. Политика безопасности в компьютерных системах. Оценка защищенности. Способы защиты конфиденциальности, целостности и доступности в КС. Стандарты и рекомендации по оценке защищенности от НСД Архитектура ЭВМ и виды современных многопользовательских и многозадачных операционных систем. Реализация подсистемы безопасности ОС. Идентификация и аутентификация пользователей ОС Контроль доступа и разграничение доступа. Дискреционное и мандатное разграничение доступа. Пользователи и группы. Файл как объект доступа. Оценка надежности систем ограничения доступа - сведение к задаче оценки стойкости. Иерархический доступ к файлу. Понятие атрибутов доступа. Защита файловых ресурсов в ОС Windows и Unix Способы исследования программ, виды отладчиков. Ресурсы, упакованные в программном модуле. Секции программ. Трассировка программ платформы Win32 и программ, платформ .NET и Java				

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 сетевых автоматизированных систем	8	0	8	20
Идентификация субъекта. Понятие протокола идентификации. Локальная и удаленная идентификация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами. Программно-аппаратные средства аутентификации: биометрические, пассивные и активные устройства. Сетевая аутентификация в корпоративных системах. Управление сертификатами Kerberos. Протокол LDAP. Инфраструктура управления ключами PKI Принципы работы и функционал СЗИ. Обеспечение безопасной загрузки операционной системы и верификация модулей. Централизованное управление. Интеграция в существующую автоматизированную систему предприятия. Средства, сертифицированные ФСТЭК. Примеры СЗИ Структура и функционал электронных ключей. Программные модули: драйвер ключа и API ключа. Структура защищенной программы. Преимущества и ограничения ключей как методы защиты ПО от нелегального распространения. Виды защиты: конверт (envelope), триальные и ограниченные версии, интеграция API ключа в разрабатываемую программу. Разрушающие программные воздействия: вирусы, трояны, malware, adware. Классификация и технологии вирусов. Руткиты: вредоносное ПО для организации удаленного управления ЭВМ и создания ботнетов IDS/IPS. Алгоритмы интеллектуального анализа сетевой и локальной активности, выявляющие нестандартный обмен информацией. Пассивное и активное обнаружение атак. Прмеры систем предотвращения вторжений: Microsoft TMG, Snort.				
Средства обеспечения информационной безопасности распределенных информационных систем	8	0	12	14
Виртуальные среды и машины: уровень интеграции виртуальной системы и совместное использование ресурсов хост-машины. Кластеры. Облачные технлогии SaaS, PaaS, IaaS и прочие. Размещение вычислительных ресурсов организации в коммерческих и свободных облачных хостингах. Экономические и правовые вопросы использования облачных технологий. Вопросы безопасности данных в виртуальных и облачных средах. Виртуальные частные сети (VPN). Программные и аппаратные средства				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
создания VPN и VLAN Аппаратаные криптошлюзы Континент и Криптон. Доступ удаленного пользователя в локальную сеть организации. Связь разбросанных филиалов организации в единую сеть. Организация межкорпоративного сетевого портала для ведения совместного проекта. Защищенный серфинг. криптографическая защита данных, передаваемых по каналам связи сетей общего пользования между составными частями VPN. Настройка приоритетов трафика. Маршрутизация трафика. Протоколирование сетевой активности. Блокировка трафика. Аудит автоматизированных информационных систем. Журналы событий в операционных системах, базах данных. Обеспечение доступности и надежного хранения корпоративных данных: резервное копирование и отказоустойчивые дисковые массивы RAID. Организация хранилища данных с использованием технологий NAS, SAN.				
ИТОГО по 7-му семестру	24	0	28	54
ИТОГО по дисциплине	24	0	28	54

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Установка и настройка средства доверенной загрузки СДЗ «Аккорд-5.5»
2	Установка и настройка средства доверенной загрузки «Аккорд-GX»
3	Установка и настройка средства защиты информации от несанкционированного доступа «Аккорд-Win64»
4	Изучение электронной подписи и шифрования файлов на примере программного обеспечения «ANCUD Crypton ArcMail»
5	Изучение электронной подписи и шифрования файлов на примере программно-аппаратного комплекса «ШИПКА»
6	Изучение шифрования трафика на примере программного обеспечения «ANCUD Crypton IPMobile»
7	Применение защищенного носителя информации на примере программно-аппаратного комплекса «Секрет особого назначения» (4 часа). организационно - техническим решениям

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.

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	Безукладников И. И., Кон Е. Л., Южаков А. А. Проектирование и эксплуатация автоматизированных систем диспетчерского управления объектами критической инфраструктуры современного города : учебное пособие для вузов. Пермь : Изд-во ПНИПУ, 2012. 174 с. 14,2 усл. печ. л.	5
2	Основы управления информационной безопасностью : учебное пособие для вузов / Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. 2-е изд., испр Москва : Горячая линия-Телеком, 2014. 243 с. 15,25 усл. печ. л.	15

3	Прокушев Я. Е. Информационная безопасность : лабораторный практикум. Санкт-Петербург : ИЦ Интермедия, 2018. 286 с. 16,74 усл. печ. л.	2
4	Хорев П. Б. Программно-аппаратная защита информации : учебное пособие для вузов. Москва : ФОРУМ, 2009. 351 с.	2
5	Хорев П. Б. Программно-аппаратная защита информации : учебное пособие для вузов. 2-е изд., испр. и доп Москва : ФОРУМ, 2015. 351 с. 22,0 усл. печ. л.	2
6	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
7	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие. М. : ФОРУМ : ИНФРА-М, 2009. 415 с.	2
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	Гаврилов М,В. Информатика и информационные технологии : учебник для бакалавров / М. В. Гаврилов, В. А. Климов .— 2-е изд., испр. и доп .— Мо-сква : Юрайт, 2012 .— 350 с., 18,38 усл. печ. л. : ил .— (Бакалавр) .— Биб-лиогр.: с. 350	3
3	Таненбаум Э. Современные операционные системы : пер. с англ. 3-е изд. Санкт-Петербург [и др.] : Питер, 2012. 1115 с. 90,300 усл. печ. л.	6
4	Таненбаум Э. Современные операционные системы : пер. с англ. 3-е изд. Санкт-Петербург [и др.] : Питер, 2015. 1115 с. 90,300 усл. печ. л.	4
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	Администрирование: Групповая политика безопасности	https://cloud.mail.ru/public/dLFr/ibo5rBQCL	сеть Интернет; свободный доступ

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Администрирование: Локальная безопасность Windows	https://cloud.mail.ru/public/BQcA/SXiJkt5Xv	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)
Прикладное программное обеспечение общего назначения	Wireshark

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

Наименование	Ссылка на информационный ресурс
База данных уязвимостей CVE Mitre	https://cve.mitre.org/
Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю	https://bdu.fstec.ru/
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
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 «Программно-аппаратные средства защиты информации»
Приложение к рабочей программе дисциплины

Направление подготовки:	10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы:	Комплексная защита объектов информатизации
Квалификация выпускника:	Бакалавр
Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация (профиль) образовательной программы:	Безопасность открытых информационных систем
Квалификация выпускника:	Специалист
Выпускающая кафедра:	Автоматика и телемеханика
Форма обучения:	Очная

Курс: 4 **Семестр**: 7

Трудоёмкость:
Кредитов по рабочему учебному плану: 3 ЗЕ
Часов по рабочему учебному плану: 108 ч.

Форма промежуточной аттестации:
Зачёт с оценкой: 7 семестр

Пермь 2023

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «**Программно-аппаратные средства защиты информации**» 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 (7-го семестра учебного плана) и разбито на 2 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные, практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются 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 зачета. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине (10.03.01)

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ОЛР**	**Т/КР**		**Зачёт**
Усвоенные знания						
З.1 Знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем		ТО1		КР1		ТВ
Освоенные умения						
У.1 Умеет анализировать программные и программно-аппаратные решения при проектировании систем защиты информации с целью выявления уязвимостей. развертывать и настраивать программные и аппаратные средства для защиты локальных и распределенных вычислительных систем				КР2		ПЗ
Приобретенные владения						
В.1 Владеет навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации			ОП31 ОП32 ОП33			

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине (10.05.03)

Контролируемые результаты обучения по дисциплине (ЗУВы)	Вид контроля					
	Текущий		Рубежный		Итоговый	
	С	ТО	ОЛР	Т/КР		Зачёт
Усвоенные знания						
З.1 Знает принципы организации, критерии оценки эффективности и надежности систем защиты информации; основные протоколы, используемые для защиты информации в вычислительных сетях и системах передачи информации		ТО1		КР1		ТВ
Освоенные умения						
У.1 Умеет развертывать и настраивать программные и аппаратные средства для защиты локальных и распределенных вычислительных систем; настраивать каналы безопасного обмена информацией в локальных и распределенных автоматизированных системах.				КР2		ПЗ
Приобретенные владения						
В.1 Владеет инструментарием, обеспечивающим программно-аппаратную защиту информационных ресурсов от изучения, модификации и копирования			ОПЗ1 ОПЗ2 ОПЗ3			

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 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 3 практических занятия (ПЗ).

Типовые темы ПЗ:

Индивидуальное задание по практическому занятию представляет собой последовательность мероприятий по настройке системы безопасности типовых локальных и распределенных автоматизированных систем. Исследование системы и необходимые способы обеспечения ее безопасности производится в соответствии с вариантом. Требования устанавливаются относительно класса защиты автоматизированной системы от несанкционированного доступа, уровня защищенности персональных данных, особенностей автоматизированной системы, а также угроз безопасности информации, характерных для данной системы. Темы работ соответствуют последовательности изучаемых тем в модулях учебной дисциплины. Выполнение работ осуществляется в среде виртуальных машин с использованием свободно распространяемых компонентов и систем.

Раздел 1, модуль 1

Тема 1. Развертывание прототипа автоматизарованной системы в виртуальной среде на базе Windows и установка операционной системы для выявления уязвимостей и реализации атак (Kali Linux).

Тема 2. Настройка сетевого взаимодействия между виртуальными машинами и установка серверного программного обеспечения на изучаемую машину.

Тема 3. Настройка локальной безопасности Windows и настройка разграничения доступа к файловым ресурсам и реестру.

Тема 4. Изучение тестового приложения в отладчике и применение патча.

Раздел 2, модуль 2

Тема 5. Настройка в виртуальной машине Active Directory и изучение LDAP. Изучение технологии RDP: удаленного рабочего стола.

Тема 6. Изучение автоматизированной системы с помощью сканера уязвимостей Nessus и выполение эксплойтов. Поиск методов устранения уязвимостей (патчей).

Тема 7. Установка демоверсии комплекса HASP и защита простой программы с помощью ключа.

Тема 8. Настройка антивируса, настройка параметров автозапуска сменных носителей, настройка прав доступа к веткам реестра, отвечающим за автоматический старт программ.

Тема 9. Настройка системы предотвращения вторжений Snort.

Раздел 3, модуль 3

Тема 10. Размещение образа автоматизированной системы в бесплатном хостинге и проверка настроек безопасности с помощью сканера портов.

Тема 11. Настройка программной VPN между удаленными системами.

Тема 12. Средства аудита и обеспечения отказоустойчивости автоматизированной системы.

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

2.2.2. Рубежная контрольная работа

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

Типовые задания КР1:

1. Выбор программно-аппаратных СЗИ и их конфигурации для защиты локальной системы.

Типовые задания КР2:

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

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 зачета. 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 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 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 зачета по дисциплине

Типовые вопросы для контроля усвоенных знаний:

Тема 1: Основные понятия и определения в сфере информационной безопасности. Угрозы информации. Анализ методов и средств защиты информации.

Тема 2: Изучение архитектуры ЭВМ и принципов выполнения программ в Фон-Неймановской архитектуре компьютера.

Тема 3: Изучение иерархической системы разграничения доступа в файловой системе и реестре ОС Windows.

Тема 4: Изучение основных команд языка Ассемблер и управления выполнением программ.

Тема 5: Аппаратные средства аутентификации с использованием биометрических данных и смарт-карт.

Тема 6: Изучение структуры типовой СЗИ Аккорд.

Тема 7: Изучение способов реализации ключевой защиты .

Тема 8: Изучение методов реализации руткитов средствами системного программного обеспечения DDK.

Тема 9: Методы обнаружения активности вредоносного ПО.

Тема 10: Изучение облачных технологий «Инфраструктура как сервис» и «Платформа как сервис».

Тема 11: Изучение методов и криптографических алгоритмов организации защищенных каналов.

Тема 12: Архивация данных Стратегии архивации

Типовые вопросы и практические задания для контроля освоенных умений:

1. Решение ситуационных задач по выбору и применению аппаратно-программных СЗИ на заданном объекте.

2.4.2.2. Шкалы оценивания результатов обучения на 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 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 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 зачета используются типовые критерии, приведенные в общей части ФОС образовательной программы.