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: Безопасность операционных систем
(наименование)

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

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

Общая трудоёмкость: 360 (10)
(часы (ЗЕ))

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем
(код и наименование направления)

Направленность: Безопасность открытых информационных систем (СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе реализации требований по правовой защите информации и организационному обеспечению информационной безопасности.

1.2. Изучаемые объекты дисциплины

ознакомление с политикой безопасности компании в области информационной безопасности; ознакомление со стандартами информационной безопасности; изучение криптографических методов и алгоритмов шифрования информации; изучение алгоритмов аутентификации пользователей; приобретение навыков защиты информации в сетях; изучение требований к системам защиты информации. приобретение умений в разработке проектов нормативных и организационно-распорядительных документов в области обеспечения информационной безопасности и их применении; приобретение навыков работы в организации и обеспечении режима секретности, физической защиты объектов, методах организации работы с персоналом и управлению деятельностью служб защиты информации на предприятии.

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-10	ИД-1ОПК-10	Знает: Виды угроз информационной безопасности. Способы и методы возможных нарушений нормального функционирования информационной системы. Программные и аппаратные методы обеспечения информационной безопасности. Информационные базы источников угроз безопасности, утвержденные в РФ. Способы обеспечения информационной безопасности в условиях функционирования в России глобальных сетей. передачи данных Виды нарушителей информационной безопасности. Модели информационной безопасности.	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	Экзамен
ОПК-10	ИД-2ОПК-10	Умеет - конфигурировать параметры программных средств защиты информации. - управлять правами пользователей. Локальная политика безопасности в Windows и Linux; - использовать программные интерфейсы и библиотеки криптопровайдеров Crypto API; - использовать Электронные ключи и смарт-карты для обеспечения разграничения доступа и шифрования..	Умеет конфигурировать параметры системы защиты информации современных операционных систем; контролировать эффективность принятых мер по реализации политик безопасности информации в современных операционных системах; проводить анализ угроз безопасности в локальных вычислительных сетях	Индивидуальное задание
ОПК-10	ИД-3ОПК-10	Владеет навыками: - формирования модели угроз безопасности	Владеет навыками формирования модели угроз безопасности	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
		информации в АИС. - анализа уязвимостей и способов нарушений информационной безопасности в АИС. - составления перечня мер и способов защиты информации - настройки и использования защищенных компьютерных систем	информации автоматизированных систем	
ОПК-12	ИД-1ОПК-12	Знает: Архитектуру операционных систем. Процесс и особенности загрузки операционных систем. Классификицию программного обеспечения. Защищенный режим работы процессора. Уровни доступа. Разграничение адресного пространства и ресурсов ПК. Драйверы. Сервисы. Утилиты. Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Модели безопасности и их применение. Таксономию нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем	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	Зачет
ОПК-12	ИД-2ОПК-12	Умеет - использовать программное	Умеет использовать средства защиты информации	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
		обеспечение шифрования данных. - использовать безопасные протоколов передачи данных. - анализировать сетевой трафик - настраивать информационную безопасность локальные и групповые политики современнх операционных систем	операционных систем; разрабатывать и администрировать базы данных	
ОПК-12	ИД-3ОПК-12	Владеет навыками - использования средства защиты информации операционных систем; - разработки и администрирования баз данных; - конфигурирования параметры системы защиты информации современных операционных систем; - контроля эффективность принятых мер по реализации политик безопасности информации в современных операционных системах; - проведения анализа угроз безопасности в локальных вычислительных сетях	Владеет навыками настройки сервисов безопасности операционных систем	Курсовая работа

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		9	10
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	144	72	72
- лекции (Л)	72	36	36
- лабораторные работы (ЛР)	32	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	36	18	18
- контроль самостоятельной работы (КСР)	4	2	2
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	180	108	72
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет	9		9
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)	18	18	
Общая трудоемкость дисциплины	360	216	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
9-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	18	0	8	54
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	18	16	10	54
Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Модели безопасности и их применение. Таксо-номия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта). За-щита информации от утечки за счет побочного электромагнитного излучения и наводок. Методы и средства защиты информации от случайных воздействий. Методы защиты инфор-мации от аварийных ситуаций. Организационные мероприятия по защите информации. Ор-ганизация информационной безопасности компании. Выбор средств информационной ин-формации. Информационное страхование				
ИТОГО по 9-му семестру	36	16	18	108
10-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
Программные методы обеспечение информационной безопасности	18	8	8	36
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 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				
Принципы разработки защищенного программного обеспечения	18	8	10	36
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 10-му семестру	36	16	18	72
ИТОГО по дисциплине	72	32	36	180

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Информационные отношения как объект правового регулирова-ния; Правовой режим защиты государственной тайны; Правовой режим защиты информации конфиденциального характера
2	Организация многорубежной системы охраны; Организация ре-жимных мероприятий

№ п.п.	Наименование темы практического (семинарского) занятия
3	Институт правовой защиты служебной тайны; Институт правовой защиты коммерческой тайны; Институт правовой защиты банковской тайны; Допуск к государственной тайне. Организация служебного расследования по фактам утраты информации
4	Модель угроз. Модель нарушителя. Классы информационных систем
5	Понятие и сущность программной защиты информации. Управление правами пользователей. Локальная политика безопасности в Windows и Linux
6	Вирусы. Руткиты. Антивирусы. Архитектура и возможности про-граммного обеспечения антивирусов. Интеграция в файловую и сетевую подсистемы.
7	Электронные ключи и смарт-карты для обеспечения разграниче-ния доступа и шифрования.
8	Программные интерфейсы и библиотеки криптопровайдеров Crypto API.

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Локальная безопасность Windows и анализ уязвимостей операци-онной системы
2	Локальная безопасность Linux и анализ уязвимостей операционной системы
3	Использование программного обеспечения шифрования данных. Использование безопасных протоколов передачи данных. Перехват трафика с использованием ПО Wireshark
4	Модели безопасности ИС и их применение
5	Централизованная настройка информационной безопасности Win-dows Active Directory и интеграция Samba Server в AD
6	Настройка типового антивируса. Обновление баз. Настройка фай-ервола. Поиск вирусной активности с использованием реестра, диспетчера процессов, файловых менеджеров
7	Установка СУБД Oracle XE на подготовленной виртуальной маши-не. Настройка автоматического резервного копирования. Перенос данных с помощью утилит экспорта/импорта. Подключение к уда-ленным БД. СУБД Oracle XE: Создание пользователей и задание привилегий. Создание пакетов процедур и триггеров на языке PL/SQL. Настройка аудита
8	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
9	Разработка приложения для работы с БД, исследование прав поль-зователей БД
10	Разработка приложения для работы с электронными ключами

Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	Разработка защищенного клиент-серверного программного обеспечения для заданной предметной области

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	Голенищев Э. П., Клименко И. В. Информационное обеспечение систем управления : учебное пособие для вузов. Ростов-на-Дону : Феникс, 2010. 315 с.	5

2	Информационная безопасность и защита информации : учебное пособие для вузов / Громов Ю. Ю., Драчёв В. О., Иванова О. Г., Шахов Н. Г. 2-е изд., перераб. и доп Старый Оскол : ТНТ, 2016. 383 с. 22,32 усл. печ. л.	2
3	Нестеров С. А. Основы информационной безопасности : учебное пособие. 3-е изд., стер Санкт-Петербург [и др.] : Лань, 2017. 321 с. 20,25 усл. печ. л.	4
4	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
5	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
6	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие. М. : ФОРУМ : ИНФРА-М, 2008. 415 с.	10
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	Олифер В.Г., Олифер Н.А. Сетевые операционные системы : учебное пособие для вузов. 2-е изд СПб : Питер, 2009. 668 с.	5
3	Т.Кайт. Oracle для профессионалов / Том Кайт Кн.2: Расширение возмож-ностей и защита .— 2-е изд. — 2004 .— 831 с	3
4	Т.Кайт. Oracle для профессионалов : пер. с англ. / Том Кайт. Кн. 1: Архи-тектура и основные особенности .— 2-е изд. — 2004 .— 662 с	3
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/xAvt/g7gQFsKVL	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
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
Курсовая работа	Персональный компьютер	12
Лабораторная работа	Персональный компьютер	12
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 «Безопасность операционных систем»
Приложение к рабочей программе дисциплины

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: 4,5 **Семестр**: 9,10

Трудоёмкость:
Кредитов по рабочему учебному плану: 10 ЗЕ
Часов по рабочему учебному плану: 360 ч.

Форма промежуточной аттестации:
Зачёт: 9 семестр Курсовая работа: 9 семестр
Экзамен: 10 семестр

Пермь 2023

Фонд оценочных средств 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 двух семестров (9-го и 10-го семестра учебного плана) и разбито на 4 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные, практические и лабораторные 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 и лабораторным работам, защита отчета по курсовой работе, зачета и экзамена. 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**	**КР**	**Зачёт/ экзамен**
Усвоенные знания						
З.1 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		ТО1		КР1, КР2		ТВ
З.2 Знает принципы организации и структуру систем защиты информации современных операционных систем; средства защиты информации систем управления базами данных;		ТО2		КР3, КР4		ТВ
Освоенные умения						
У.1 Умеет использовать средства защиты информации операционных систем; разрабатывать и администрировать базы данных.			ОПЗ1 ОПЗ2 ОПЗ3 ОПЗ4			ПЗ
У.2 Умеет проводить установку и настройку современных операционных систем с учетом требований по обеспечению информационной			ОПЗ5 ОПЗ6 ОПЗ7			ПЗ

безопасности; восстанавливать операционные системы после сбоев; реализовывать политику безопасности в локальной вычислительной сети; конфигурировать средства защиты информации систем управления базами данных						
Приобретенные владения						
В.1 Владеет навыками настройки сервисов безопасности операционных систем			ОЛР1 ОЛР2 ОЛР3 ОЛР4 ОЛР5		КР	
В.2 Владеет навыками использования средств операционных систем для обеспечения безопасного функционирования автоматизированных систем			ОЛР6 ОЛР7 ОЛР8 ОЛР9 ОЛР10		КР	

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; ОПЗ – отчет по практическому заданию; Т/КР – рубежное тестирование (контрольная работа); ТВ – теоретический вопрос; КР – отчет по курсовой работе; 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 лабораторным и практическим работам, 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 лабораторных работ и рубежных контрольных работ (после проведения практических занятий).

2.2.1. Защита лабораторных работ

Всего запланировано 10 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Наименование темы лабораторной работы

1 Локальная безопасность Windows и анализ уязвимостей операционной системы

2 Локальная безопасность Linux и анализ уязвимостей операционной системы

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

4 Модели безопасности ИС и их применение

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

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

7 Установка СУБД Oracle XE на подготовленной виртуальной машине. Настройка автоматического резервного копирования. Перенос данных с помощью утилит экспорта/импорта. Подключение к удаленным БД. СУБД Oracle XE: Создание пользователей и задание привилегий. Создание пакетов процедур и триггеров на языке PL/SQL. Настройка аудита

8 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

9 Разработка приложения для работы с БД, исследование прав пользователей БД

10 Разработка приложения для работы с электронными ключами

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

2.2.2. Защита отчетов по практическим занятиям

Всего запланировано 7 практических занятия. Типовые темы ПЗ приведены в РПД.

Наименование темы практического (семинарского) занятия

1 Организация многорубежной системы информационной безопасности
2 Организация служебного расследования по фактам утраты информации
3 Модель угроз. Модель нарушителя. Классы информационных систем
4 Понятие и сущность программной защиты информации. Управление правами пользователей. Локальная и групповая политика безопасности в Windows и Linux
5 Вирусы. Руткиты. Антивирусы. Архитектура и возможности программного обеспечения антивирусов. Интеграция в файловую и сетевую подсистемы.
6 Электронные ключи и смарт-карты для обеспечения разграничения доступа и шифрования.
7 Программные интерфейсы и библиотеки криптопровайдеров Crypto API.

Защита ОПЗ 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

Типовые задания КР3:

1. Локальные политики безопасности ОС
2. Групповые политики безопасности ОС

Типовые задания КР4:

1. Организация многорубежной системы информационной безопасности
2. Организация служебного расследования по фактам утраты информации

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

2.3. Выполнение курсовой работы

Для оценивания навыков и опыта деятельности (владения), как результата обучения по дисциплине, студенты выполняют и защищают отчет по курсовой работе.

Типовые темы курсовых проектов/работ

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

2. Проведение исследования защищенности локальных и распределенных АИС, применение и настройка средств и мер обеспечения информационной безопасности

Типовые шкала и критерии оценки результатов защиты индивидуального комплексного задания приведены в общей части ФОС образовательной программы.

2.4. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных и практических работ, защита курсовой работы 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 в 9м семестре и экзамена в 10м семестре. Зачет по дисциплине основывается на результатах выполнения предыдущих индивидуальных заданий студента по данной дисциплине и курсовой работы. Экзамен проводится 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.

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 или экзамена 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 экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1 Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Модели безопасности и их применение.

2 Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
3 Анализ способов нарушений информационной безопасности.
4 Архитектура операционных систем. Процесс загрузки операционных систем. Классификиция программного обеспечения.
5 Защищенный режим работы процессора. Уровни доступа. Разграничение адресного пространства и ресурсов ПК.
6 Драйверы. Сервисы. Утилиты
7 Методы криптографии. Классификация криптографических методов. Характеристики существующих шифров. Кодирование.
8 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.
10 Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы
11 Принципы разработки защищенного программного обеспечения. Виды угроз. Разграничение доступа к ресурсам ИС.
12 Идентификация и аутентификация пользователей в ОС семейства Windows и Linux.
13 Аудит событий безопасности.
14 Администрирование прав пользователей.
15 Аппаратно-программные комплексы обеспечения безопасности ОС
16 Управление доступом к ресурсам в программном коде. Получение информации об идентификации и аутентификации пользователей в ОС семейства Windows и Linux.
17 Использование встроенных API шифрования Crypto API.
18 Исследование программного кода для работы с электронными ключами
19 Использование защищенных компьютерных систем. Методы обеспечения информационной безопасности в РФ.
20 Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ.
21 Идентификация и установление подлинности объекта (субъекта). Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Методы и средства защиты информации от случайных воздействий.
22 Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации.
23 Организация информационной безопасности компании. Выбор средств информационной информации. Информационное страхование

Типовые вопросы и практические задания для контроля освоенных умений:

1. Классификация информационной системы и обоснование требований ИБ.

2. Разработка модели угроз и модели нарушителя.

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

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.