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
« 09 » октября 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Защищенные информационные системы
(наименование)

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

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

Общая трудоёмкость: 180 (5)
(часы (ЗЕ))

Направление подготовки: 10.04.01 Информационная безопасность
(код и наименование направления)

Направленность: Комплексные системы информационной безопасности
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель дисциплины - освоение дисциплинарных компетенций, связанных с созданием и изучением современной защищенных информационных систем различного применения и степени сложности.
Задачи дисциплины:
- изучение современной классификации средств защиты информации в корпоративных вычислительных сетях и системах;
- изучение современных технологий построения безопасных информационных систем;
- изучение этапов и технологий проектирования и создания безопасных информационных систем;
- изучение современных программных и аппаратных средств защиты информации;
- изучение основных угроз информации в современных информационных системах и сетях;
- изучение инструментальных программных и аппаратных средств анализа защищенности информационных систем и сетей;
- формирование умений в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации;
- формирование навыков разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов.

1.2. Изучаемые объекты дисциплины

- методы и средства защиты информации в корпоративных вычислительных сетях и системах;
- основные угрозы информации в современных сложных сетевых информационных системах;
- программные, программно-аппаратные и аппаратные средства защиты информации, применяемые при обеспечении комплексной информационной безопасности;
- программные средства анализа текущего уровня защищенности;
- современные технологии построения безопасных информационных систем и сетей.

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-1	ИД-1ОПК-1	Знает направления развития и проблемы компьютерного моделирования распределенных информационных систем	Знает направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем	Отчёт по практическом у занятию
ОПК-1	ИД-2ОПК-1	Умеет обосновывать и планировать состав и архитектуру моделируемых информационных систем.	Умеет обосновывать и планировать состав и архитектуру моделируемых сложных систем; обосновывать и планировать состав и архитектуру проектируемых информационных, автоматизированных и автоматических систем.	Защита лабораторной работы
ОПК-1	ИД-3ОПК-1	Владеет навыками разработки концептуальных стратегий решения задач моделирования и проектирования распределенных информационных систем и систем обеспечения ИБ	Владеет навыками навыками разработки концептуальных стратегий решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения ИБ.	Курсовая работа
ОПК-2	ИД-1ОПК-2	Знает методы концептуального проектирования технологий обеспечения информационной безопасности.	Знает методы концептуального проектирования технологий обеспечения информационной безопасности.	Отчёт по практическом у занятию
ОПК-2	ИД-2ОПК-2	Умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.	Защита лабораторной работы
ОПК-2	ИД-3ОПК-2	Владеет средствами автоматизированного тестирования систем защиты информации	Владеет средствами автоматизи-рованного и ручного функцио-нального тестирования.	Курсовая работа
ПКО-2	ИД-1ПКО-2	Знает подходы к построению и	Знает подходы к построению и	Отчёт по практическо

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		исследованию моделей процессов защиты информации в распределенных информационных системах	исследованию моделей процессов защиты информации в автоматизи-рованных системах	му занятию
ПКО-2	ИД-2ПКО-2	Умеет разрабатывать и доказывать адекватность моделей систем защиты информации	Умеет разрабатывать и доказывать адекватность моделей систем защиты информации	Защита лабораторной работы
ПКО-2	ИД-3ПКО-2	Владеет навыками применения программного обеспечения в задачах моделирования и исследования моделей систем защиты информации	Владеет навыками применения программного обеспечения в задачах моделирования и исследования моделей систем защиты информации	Курсовая работа

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		2
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	83	83
- лекции (Л)	18	18
- лабораторные работы (ЛР)	24	24
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	36	36
- контроль самостоятельной работы (КСР)	5	5
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	61	61
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)	18	18
Общая трудоемкость дисциплины	180	180

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
2-й семестр				
Цель проекта информационной безопасности	2	0	2	4
Цель и задачи проекта. Требования регуляторов. Сохранение информации. Вы-явление источников и каналов утечки информации. Системный ландшафт. Права пользователей. Квалификация пользователей. Средства защиты.				
Локализация задачи. Способы хранения конфиденциальной информации	2	0	2	4
Локализация задачи. Положение о конфиденциальной информации в электронном виде. Контентная категоризация. Классификация информации по уровню конфиденциальности. Метки документов. Хранение информации. Способы хранения конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация. Локальные копии				
Основные направления защиты. Классификация внутренних нарушителей	2	0	2	4
Основные направления защиты. Защита документов. Защита каналов утечки. Мониторинг (аудит) действий пользователей. Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные. Нарушители, мотивированные из-вне. Другие типы нарушителей				
Нетехнические меры защиты. Уровни контроля информационных потоков	0	0	4	5
Нетехнические меры защиты от внутренних угроз. Психологические меры. Органи-зационные меры. Права локальных пользователей. Стандартизация ПО. Специфические решения. Работа с кадрами. Хранение физических носителей. Уровни контроля информационных потоков. Режим архива. Режим сигнализации. Режим активной защиты				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Классификация firewall'ов и определение политики firewall'а	2	6	2	4
Классификация firewall'ов. Установление TCP-соединения. Пакетные фильтры. По-граничные роутеры. Пример набора правил пакетного фильтра. Stateful Inspection firewall'ы. Host-based firewall'ы. Персональные firewall'ы и персональные устройства firewall'а. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Гибридные технологии firewall'а. Трансляция сетевых адресов (NAT). Статическая трансляция сетевых адресов. Скрытая трансляция сетевых адресов				
Различные типы окружений firewall'а	2	0	2	4
Принципы построения окружения firewall'а. DMZ-сети. Конфигурация с одной DMZ-сетью. Service Leg конфигурация. Конфигурация с двумя DMZ-сетями. Виртуальные частные сети. Расположение VPN-серверов. Интранет. Экстранет. Компоненты инфра-структуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях. Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы. SMTP-серверы. Политика безопасности firewall'а. Политика firewall'а. Реализация набора правил firewall'а. Тестирование политики firewall'а. Возможные подходы к эксплуатации firewall'а. Сопровождение firewall'а и управление firewall'ом. Физическая безопасность ок-ружения firewall'а. Администрирование firewall'а. Встраивание firewall'ов в ОС. Стратегии восстановления после сбоев firewall'а. Возможности создания логов firewall'а. Инциденты безопасности. Создание backup'ов firewall'ов				
Пример пакетных фильтров в ОС FreeBSD 6.0	2	0	2	4
Основные характеристики пакетных фильтров в ОС FreeBSD. ПО пакетных фильтров. OpenBSD Packet Filter (PF) и ALTQ. Указание необходимости использования PF. Оп-ции ядра. Опции rc.conf. Указание необходимости использования ALTQ. Создание правил фильтрации. IPFILTER (IPF) firewall. Указание необходимости использования IPF. Опции ядра. Опции, доступные в rc.conf. Построение скрипта правил с использованием символьных подстановок. Набор правил IPF. Трансляция сетевых адресов(NAT).NAT для очень больших LAN. Использование пула публичных адресов. Port Redirection				
Системы обнаружения атак (Intrusion Detection Systems, IDS)	0	0	2	5

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Понятие системы обнаружения атак. Почему следует использовать IDS. Типы IDS. Базовая архитектура IDS. Совместное расположение Host и Target. Разделение Host и Target. Способы управления IDS. Централизованное управление. Частично распределенное управление. Полностью распределенное управление. Скорость реакции. Информационные источники. Network-Based IDS. Host-Based IDS. Application-Based IDS. Анализ, выполняемый IDS. Определение злоупотреблений. Определение аномалий. Возможные ответные действия IDS. Активные действия. Сбор дополнительной информации. Изменение окружения. Выполнение действия против атакующего. Пассивные действия. Тревоги и оповещения. Использование SNMP Traps. Возможности отчетов и архивирования. Возможность хранения информации о сбоях. Дополнительные инструментальные средства. Системы анализа и оценки уязвимостей. Процесс анализа уязвимостей. Классификация инструментальных средств анализа уязвимостей. Host-Based анализ уязвимостей. Network-Based анализ уязвимостей. Преимущества и недостатки систем анализа уязвимостей. Способы взаимодействия сканера уязвимостей и IDS. Проверка целостности файлов				
Развертывание систем обнаружения атак на предприятии	0	6	4	4
Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS. Цели и задачи использования IDS. Существующая политика безопасности. Организационные требования и ограничения. Ограничения на ресурсы, существующие в организации. Возможности IDS. Учет возможного роста организации. Предоставляемая поддержка программного продукта. Развертывание IDS. Стратегия развертывания IDS. Развертывание network-based IDS. Обработка выходной информации IDS. Типичные выходные данные IDS. Выполняемые IDS действия при обнаружении атаки. Компьютерные атаки и уязвимости, определяемые IDS. Типы компьютерных атак, обычно определяемые IDS. Определение расположения атакующего на основе анализа выходной информации IDS				
Безопасное использование службы доменных имен (DNS)	2	6	4	4
Безопасность DNS. Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
для них. Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS. Зонный файл. Name-серверы. Авторитетные name-серверы. Кэширующие name-серверы. Resolver'ы. Транзакции DNS. Запрос / ответ DNS. Зонная пересылка. Динамические обновления. DNS NOTIFY. Безопасность окружения DNS. Угрозы и обеспечение защиты платформы хоста. Угрозы ПО DNS. Угрозы для данных DNS.				
Обеспечение безопасности web-серверов	2	0	2	5
Причины уязвимости web-сервера. Планирование развертывания web-сервера. Безопасность лежащей в основе ОС. Безопасное инсталлирование и конфигурирование ОС. Применение Patch и Upgrade ОС. Удаление или запрещение ненужных сервисов и прило-жений. Конфигурирование аутентификации пользователя в ОС. Управление ресурсами на уровне ОС. Альтернативные платформы для web-сервера. Trusted ОС. Использование Appliances для web-сервера. Специально усиленные (pre-hardened) ОС и web-серверы. Тестирование безопасности операционной системы. Список действий для обеспечения безо-пасности ОС, на которой выполняется web-сервер. Безопасное инсталлирование и конфигурирование web-сервера. Безопасное инсталлирование web-сервера. Конфигурирование управления доступом. Разграничение доступа для ПО web-сервера. Управление доступом к директории содержимого web-сервера. Управление влиянием web Bots. Использование программ проверки целостности файлов. Список действий для безопасного инсталлирования и конфигурирования web-сервера				
Безопасность web-ориентированного контента	2	0	2	4
Опубликование информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера. Список действий для обеспечения безопасности web-содержимого				
Технологии аутентификации и шифрования	0	0	2	5
Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация. SSL/TLS. Возможности SSL/TLS. Слабые места SSL/TLS. Пример SSL/TLS-сессии. Схемы шифрования SSL/TLS. Требования к реализации SSL/TLS. Список действий для технологий аутентификации				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
и шифрования. Firewall прикладного уровня для web — ModSecurity. Взаимодействие ModSecurity с пакетным фильтром				
Реализация комплексной безопасной сетевой инфраструктуры для web-сервера	0	6	4	5
Топология сети. Демилитаризованная зона. Хостинг во внешней организации. Сетевые элементы. Роутер и firewall. Системы обнаружения проникновения (IDS). Сетевые коммутаторы и концентраторы. Список действий для обеспечения безопасности сетевой инфраструктуры. Администрирование web-сервера. Создание логов. Основные возможно-сти создания логов. Дополнительные требования для создания логов. Возможные параметры логов. Просмотр и хранение лог-файлов. Автоматизированные инструментальные сред-ства анализа лог-файлов. Процедуры создания backup web-сервера. Политики и стратегии выполнения backup'а web-сервера. Поддержка тестового web-сервера. Поддержка аутен-тичной копии web-содержимого. Восстановление при компрометации безопасности. Тестирование безопасности web-серверов. Сканирование уязвимостей. Тестирование проникновения. Удаленное администрирование web-сервера. Список действий для безопасного администрирования web-сервера				
ИТОГО по 2-му семестру	18	24	36	61
ИТОГО по дисциплине	18	24	36	61

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Выявление источников угроз и каналов утечки информации
2	Способы хранения конфиденциальной информации
3	Классификация внутренних нарушителей
4	Нетехнические меры защиты от внутренних угроз
5	Классификация firewall'ов
6	Принципы построения окружения firewall'а
7	Построение скрипта правил с использованием символьных подстановок
8	Системы обнаружения атак (Intrusion Detection Systems, IDS)
9	Типы компьютерных атак, обычно определяемые IDS

№ п.п.	Наименование темы практического (семинарского) занятия
10	Безопасное использование службы доменных имен (DNS)
11	Обеспечение безопасности web-серверов
12	Безопасность web-ориентированного контента
13	Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация. SSL/TLS
14	Сканирование уязвимостей. Тестирование проникновения. Удаленное администрирование web-сервера

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Настройка политики безопасности firewall’a
2	Развертывание интерактивных детекторов атак на виртуально-физической инфраструктуре XenServer
3	Развертывание основных механизмов безопасности для сервисов DNS
4	Запуск и настройка защищенного web-сервера на основе пакета LAMP

Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	Создание защищенной инфраструктуры на базе ОС Linux, с использованием ПО IPCop
2	Создание защищенной инфраструктуры на базе ОС Linux, с использованием ПО Shorewall
3	Создание защищенной инфраструктуры на базе ОС Linux, с использованием ПО Uncomplicate Firewall
4	Создание защищенной инфраструктуры на базе ОС Unix Freebsd, с использованием ПО pfSense
5	Создание защищенной инфраструктуры на базе ОС Unix Freebsd, с использованием ПО m0n0wall
6	Создание защищенной инфраструктуры на базе ОС Unix Freebsd, с использованием ПО OpenBSD PF
7	Создание защищенной инфраструктуры на базе ОС Windows, с использованием ПО Zone Alarm
8	Создание защищенной инфраструктуры на базе ОС Windows, с использованием ПО Comodo Firewall
9	Создание защищенной инфраструктуры на базе ОС Windows, с использованием ПО Kaspersky Internet Security
10	Создание защищенной инфраструктуры на базе ОС Windows, с использованием ПО Zone Alarm
11	Создание защищенной инфраструктуры на базе ОС Windows, с использованием ПО Panda Firewall
12	Создание защищенной инфраструктуры на базе ОС Windows, с использованием брандмауэра Windows Server 2012

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой 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 установления 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	Завгородний В. И. Комплексная защита информации в компьютерных системах : учебное пособие для вузов / В. И. Завгородний. - Москва: Логос, 2001.	27
2	Соколов А. В. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. - Москва: ДМК, 2002.	2

2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Малюк А. А. Введение в защиту информации в автоматизированных системах : учебное пособие для вузов / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - Москва: Горячая линия-Телеком, 2001.	11
2	Скабцов Н. В. Аудит безопасности информационных систем / Н. В. Скабцов. - Санкт-Петербург [и др.]: Питер, 2018.	2
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	Безопасность компьютерных систем	https://habr.com/ru/company/ua-hosting/blog/434342/	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	Windows 10 (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

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

Наименование	Ссылка на информационный ресурс
Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю	https://bdu.fstec.ru/

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/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Курсовая работа	Персональный компьютер	10
Лабораторная работа	Персональный компьютер	10
Лекция	Мультимедийный проектор	1
Практическое занятие	Персональный компьютер	10

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 «Защищенные информационные системы»
Приложение к рабочей программе дисциплины

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) образовательной программы: Комплексные системы информационной безопасности

Квалификация выпускника: Магистр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 1 **Семестр**: 2

Трудоёмкость:
Кредитов по рабочему учебному плану: 5 ЗЕ
Часов по рабочему учебному плану: 180 ч.

Форма промежуточной аттестации:
Экзамен: 2 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 одного семестра (2-го семестра учебного плана) и разбито на 3 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 лабораторным работам 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**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 Знает методы концептуального проектирования технологий обеспечения информационной безопасности		ТО1				КЗ
З.2 Знает подходы к построению и исследованию моделей процессов защиты информации в распределенных информационных системах		ТО2				КЗ
З.3 Знает направления развития и проблемы компьютерного моделирования распределенных информационных систем		ТО2				КЗ
Освоенные умения						
У.1 Умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью			ОЛР1 ОЛР2 ОЛР3 ОЛР4	КР		
У.2 Умеет разрабатывать и доказывать адекватность моделей систем защиты информации			ОЛР1 ОЛР2 ОЛР3 ОЛР4	КР		
У.3 Умеет обосновывать и планировать состав и архитектуру моделируемых информационных систем			ОЛР1 ОЛР2 ОЛР3 ОЛР4	КР		

Приобретенные владения						
В.1 Владеет навыками разработки концептуальных стратегий решения задач моделирования и проектирования распределенных информационных систем и систем обеспечения ИБ			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
В.2 Владеет навыками применения программного обеспечения в задачах моделирования и исследования моделей систем защиты информации			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
В.3 Владеет средствами автоматизированного тестирования систем защиты информации			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, 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 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 на групповых (практических) занятиях. 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 (после изучения каждого модуля учебной дисциплины) и курсовой работы (после изучения всех модулей учебной дисциплины).

Всего запланировано 4 лабораторных работы. Типовые темы лабораторных работ приведены в РПД.

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

Темы курсовой работы приведена в РПД. Курсовая работа содержит комплексное практическое задание по одной из выбранных тем.

Защита курсовой работы проводится индивидуально каждым студентом путем собеседования по расчетной части и демонстрации результатов разработки программной модели. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

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

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Основные понятия, термины и определения. Предмет и задачи дисциплины.
2. Анализ угроз информационной безопасности компьютерных систем.
3. Информационная безопасность в проекции на семиуровневую модель ISO OSI

4. Информационная безопасность технологий физического уровня
5. Информационная безопасность технологий канального уровня
6. Информационная безопасность технологий сетевого и транспортного уровня
7. Информационная безопасность технологий сеансового уровня
8. Информационная безопасность технологий представительского и прикладного уровня
9. Внешние (внутренние) источники угроз информационной безопасности государства.
10. Актуальные проблемы безопасности компьютерных систем.
11. Актуальные проблемы информационной безопасности при использовании мобильных средств связи.
12. Актуальные проблемы информационной безопасности в социальных сетях.
13. Актуальные проблемы информационной безопасности критически важных объектов.
14. Права пользователей. Квалификация пользователей.
15. Средства защиты. Основные направления защиты. Защита документов. Защита каналов утечки.
16. Показатели защищенности средств вычислительной техники от НСД к информации.
17. Пароль как средство защиты от НСД.
18. Требования по защите информации в автоматизированных системах от НСД.
19. Оценка безопасности информационных технологий по Общим критериям.
20. Мониторинг (аудит) действий пользователей.
21. Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные.
22. Нарушители, мотивированные извне. Другие типы нарушителей
23. Нетехнические меры защиты от внутренних угроз.
24. Психологические меры. Организационные меры.
25. Права локальных пользователей.
26. Стандартизация ПО. Специфические решения. Работа с кадрами. Хранение физических носителей.
27. Уровни контроля информационных потоков. Режим архива. Режим сигнализации. Режим активной защиты
28. Идентификация и аутентификация как сервисы безопасности.
29. Управление доступом и его виды.
30. Авторизация как сервис безопасности.
31. Протоколирование и аудит как сервисы безопасности.
32. Криптографические сервисы безопасности.
33. Классификация firewall’ов. Установление TCP-соединения. Пакетные фильтры. Пограничные роутеры.

34. Пример набора правил пакетного фильтра. Stateful Inspection firewall’ы. Host-based firewall’ы. Персональные firewall’ы и персональные устройства firewall’a.

35. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Гибридные технологии firewall’a.

36. Трансляция сетевых адресов (NAT). Статическая трансляция сетевых адресов. Скрытая трансляция сетевых адресов

37. Понятие системы обнаружения атак. Почему следует использовать IDS. Типы IDS. Базовая архитектура IDS. Совместное расположение Host и Target. Разделение Host и Target.

38. Способы управления IDS. Централизованное управление. Частично распределенное управление. Полностью распределенное управление. Скорость реакции. Информационные источники.

39. Net-work-Based IDS. Host-Based IDS. Application-Based IDS. Анализ, выполняемый IDS. Определение злоупотреблений.

40. Определение аномалий. Возможные ответные действия IDS. Активные действия.

Типовые вопросы и практические задания для контроля освоенных умений:

1. Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные. Нарушители, мотивированные извне.
2. Нетехнические меры защиты от внутренних угроз.
3. Классификация инструментальных средств анализа уязвимостей.
4. Типы компьютерных атак, обычно определяемые IDS.
5. Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация SSL/TLS.
6. Анализ базовых принципов построения защищенной мультисер-висной сети.
7. Методы анализа уровня защищенности мультисервисной сети.
8. Создание защищенной инфраструктуры веб-сервера.

2.3.2. Шкалы оценивания результатов обучения на экзамене

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

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена 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 экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

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 экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.