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

« 10 » октября 20 23 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Дисциплина:** Безопасность вычислительных сетей
(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

Цель дисциплины – формирование у студентов компетентности в области информационной безопасности вычислительных сетей.

Задачи дисциплины:

- изучение базовой инфраструктуры инфокоммуникационных сетей, основных устройств и систем, требований к обеспечению информационной безопасности, соответствующих стандартов, технических спецификаций, протоколов и технологий;
- формирование умений по созданию, настройке и эксплуатации безопасных вычислительных сетей
- овладение навыками по использованию компонентов защищенных вычислительных сетей, способностью разрабатывать модели угроз и модели нарушителей ИБ на основе исходных данных о сети

### 1.2. Изучаемые объекты дисциплины

- принципы построения защищенных компьютерных телекоммуникационных сетей;
- методы и проблемы оценивания угроз безопасности, угрозы безопасности, стандарты информационной безопасности;
- классификация типовых угроз информационной безопасности для вычислительных сетей;
- требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;
- модели и теоремы безопасности на основе дискреционной политики, модели и теоремы безопасности на основе мандатной политики;
- скрытые каналы утечки информации, модели и механизмы обеспечения целостности данных;
- нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты;
- типовые аппаратные и программные средства обеспечения информационной безопасности вычислительных 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-10 | ИД-1ОПК-10 | Знает принципы организации и структуру систем защиты информации, основные протоколы, используемые для защиты информации в вычислительных сетях, основные криптографические методы, используемые для защиты информации в вычислительных сетях | 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 | Отчёт по практическому занятию |
| ОПК-10 | ИД-2ОПК-10 | Умеет конфигурировать параметры системы защиты информации, контролировать эффективность принятых мер по реализации политик безопасности информации, проводить анализ угроз безопасности в локальных вычислительных сетях | 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 | Защита лабораторной работы |
| ОПК-10 | ИД-3ОПК-10 | Владеет навыками формирования модели угроз безопасности информации вычислительных сетей | Владеет навыками формирования модели угроз безопасности информации автоматизированных систем | Защита лабораторной работы |
| ОПК-12 | ИД-1ОПК-12 | Знает принципы построения и функционирования локальных и глобальных вычислительных сетей; последовательность и содержание этапов построения локальных вычислительных сетей; принципы построения и функционирования | Знает принципы построения и функционирования локальных и глобальных вычислительных сетей; последовательность и содержание этапов построения локальных вычислительных сетей; принципы построения и функционирования, примеры реализаций | 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 |
|---|---|---|---|---|
| | | | современных операционных систем; принципы построения и функционирования, примеры реализаций современных систем управления базами данных | |
| ОПК-12 | ИД-2ОПК-12 | Умеет использовать средства защиты информации вычислительных сетей | Умеет использовать средства защиты информации операционных систем; разрабатывать и администрировать базы данных | Защита лабораторной работы |
| ОПК-12 | ИД-3ОПК-12 | Владеет навыками настройки сервисов безопасности в вычислительных сетях | Владеет навыками настройки сервисов безопасности операционных систем | Защита лабораторной работы |

## 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:<br>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 | | | | |
| Введение в дисциплину «Безопасность вычислительных сетей» | 2 | 0 | 2 | 18 |
| Основные понятия, термины и определения. Предмет и задачи дисциплины «Безопасность вычислительных сетей» | | | | |
| Защищенные компьютерные и телекоммуникационные сети | 8 | 4 | 4 | 22 |
| Структура узлов ЗТКС. Основные принципы построения узлов связи как стационарных, так и полевых. Оперативно-технические службы узлов связи и их взаимодействие. Обеспечение и поставка техники на узлы связи. Хранение техники на узлах связи. Возможные каналы утечки информации при эксплуатации узлов ЗТКС. Основные каналы утечки информации. Методы технической защиты абонентских и соединительных линий на узлах связи. Методы защиты информации на элементах узлов связи ЗТКС | | | | |
| Основные понятия о надежности систем ЗКТС | 8 | 4 | 4 | 22 |
| Основы теории надежности систем связи. Факторы, влияющие на надежность защищенных телекоммуникационных систем; модели надежности; оценка показателей надежности; методы обеспечения надежности; влияние челове-ческого фактора на надежность защищенных телекоммуникационных систем; испытания систем на надежность | | | | |
| Угрозы безопасности в компьютерных системах | 8 | 4 | 4 | 22 |
| Понятие угрозы. Угрозы безопасности информации в компьютерных системах. Понятия "идентификация", "аутентификация", "авторизация", "спе-цификация", "классификация", "категорирование" и "каталогизация". Класси-фикационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации — критерии выделения и таксономия классов (алгебраическая полнота в операциях пересечения и объединения классов). Примеры и проблемы теоретического обоснования каталогов угроз по зарубежным, отечественным и международным стандартам | | | | |

| Наименование разделов дисциплины с кратким содержанием | Объем аудиторных занятий по видам в часах | | | Объем внеаудиторных занятий по видам в часах |
|---|---|---|---|---|
| | Л | ЛР | ПЗ | СРС |
| Политика и модели безопасности в компьютерных системах | 10 | 4 | 4 | 24 |
| Понятие политики безопасности. Модель безопасности как формализо-ванное выражение политики безопасности. Модель безопасности как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС. Составляющие модели безопасности — модель (формализация) компьютерной системы в аспекте безопасности информации, критерии, формализованные правила, алгоритмы, механизмы безопасного функционирования КС. Класс моделей конечных состояний | | | | |
| ИТОГО по 9-му семестру | 36 | 16 | 18 | 108 |
| 10-й семестр | | | | |
| Модели безопасности на основе дискреционной и мандатной политик | 8 | 4 | 4 | 18 |
| Общая характеристика политики дискреционного доступа. Тройки доступа: субъект-операция-объект. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа. Пятимерное пространство Хартсона как пример выражения дискреционного разграничения доступа на языке реляционной алгебры. Модели разграничения доступа на основе матрицы доступа. Принудительный и добровольный принцип управления доступом. Администраторы системы и владельцы объектов. Привилегии и предоставление (распространение) прав доступа. Общая характеристика политики мандатного (полномочного) доступа. Парадигма градуированного доверия пользователям (субъектам доступа) и градуированной степени конфиденциальности данных (объектов доступа). Уровни безопасности субъектов и объектов доступа. Правила безопасного мандатного доступа — запрет чтения вверх (NRU) и запрет записи вниз (NWD). Рефрексивность, антисимметричность и транзитивность отношений доступа. Функция уровня безопасности субъектов и объектов доступа | | | | |
| Модели безопасности на основе тематической и ролевой политик | 8 | 4 | 4 | 18 |
| Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств. | | | | |

| Наименование разделов дисциплины с кратким содержанием | Объем аудиторных занятий по видам в часах | | | Объем внеаудиторных занятий по видам в часах |
|---|---|---|---|---|
| | Л | ЛР | ПЗ | СРС |
| Критерии безопасности информационных потоков в системах тематического разграничения доступа. Общая характеристика политики ролевого (типизованного) доступа. Роль как типовой субъект доступа (функционально обособленное агрегирование прав доступа и полномочий выполнения процедур над данными). Две фазы организации ролевого доступа — создание ролей как типовых субъектов доступа с наделением их правами (полномочиями) доступа на основе дискреционной, мандатной, тематической или иной политики безопасности и назначение ролей пользователям | | | | |
| Межсетевые экраны, пакетная фильтрация и обнаружение атак | 10 | 4 | 4 | 18 |
| Классификация firewall'ов. Установление TCP-соединения. Пакетные фильтры. Пограничные роутеры. Пример набора правил пакетного фильтра. Stateful Inspection firewall'ы. Host-based firewall'ы. Персональные firewall'ы и персональные устройства firewall'а. Основные характеристики пакетных фильтров в ОС FreeBSD. ПО пакетных фильтров. OpenBSD Packet Filter (PF) и ALTQ. Указание необходимости использования PF. Опции ядра. Опции rc.conf. Указание необходимости использования ALTQ. Создание правил фильтрации. IPFILTER (IPF) firewall. 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 | | | | |
| Технологии обеспечения комплексной безопасности сетевых инфраструктур | 10 | 4 | 6 | 18 |
| 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 возможности создания логов. Дополнительные требования для создания логов. Возможные параметры логов. Просмотр и хранение лог-файлов. Автоматизированные инструментальные средства анализа лог-файлов. Процедуры создания backup web-сервера. | | | | |

| Наименование разделов дисциплины с кратким содержанием | Объем аудиторных занятий по видам в часах | | | Объем внеаудиторных занятий по видам в часах |
|---|---|---|---|---|
| | Л | ЛР | ПЗ | СРС |
| 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 и шифрования | | | | |
| 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 | Модель безопасности как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС |
| 2 | Тематические решетки на основе классификационных множеств |
| 3 | Сеансовая авторизация пользователя с одной или группой назначенных ему в системе ролей и доступ к объектам системы в соответствующей (соответствующих) роли (ролях) |
| 4 | Порядковое (ранговое) шкалирование компьютерных систем в аспекте безопасности на основе группирования (классификации) в пространстве шкалирования первичных факторов оценки |

Тематика примерных лабораторных работ

| № п.п. | Наименование темы лабораторной работы |
|---|---|
| 1 | Исследование каналов утечки информации в ЗКТС на примере по-левой шины LonWorks и универсальной технологии Ethernet |
| 2 | Анализ типовых факторов, влияющих на защищенность и надеж-ность ЗКТС |
| 3 | Создание классификационного перечня угроз для исследуемой лабораторной сети |
| 4 | Политики безопасности в ОС Linux, ОС Windows. Ядро операционной системы |
| 5 | Имплементация дискреционного доступа в ОС Linux |
| 6 | Имплементация мандатного доступа в ОС Linux |
| 7 | Создание элементов политики тематического доступа на базе ОС Linux и Qt Creator |
| 8 | Установка и настройка корпоративного сетевого экрана pfSense |
| 9 | Установка и настройка интерактивного детектора атак (IDS) в ОС Linux |
| 10 | Настройка SSL/TLS аутентификации при Web-доступе с использованием сервера Apache |

Тематика примерных курсовых проектов/работ

| № п.п. | Наименование темы курсовых проектов/работ |
|---|---|
| 1 | Комплексное обеспечение информационной безопасности лабора-торной инфраструктуры с использованием ОС Windows и персо-нальных решений |
| 2 | Комплексное кроссплатформенное обеспечение информационной безопасности многосегментной лабораторной сети для рабочих мест с ОС Linux, ОС Windows |

## 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 | Алгоритмы телекоммуникационных сетей Процедуры, диагностика, безопасность. Москва : ИНТУИТ, 2007. 511 с. | 7 |
| 2 | Максим М., Поллино Д. Безопасность беспроводных сетей : пер. с англ. Москва : АйТи : ДМК, 2004. 281 с. | 10 |
| 3 | Мельников В. П., Куприянов А. И., Васильева Т. Ю. Информационная безопасность : учебник для вузов. Москва : Русайнс, 2017. 354 с. 22,5 усл. печ. л. | 2 |
| 4 | Мэйволд Э. Безопасность сетей : [самоучитель пер. с англ.]. М. : СП ЭКОМ : БИНОМ. Лаб. знаний, 2005. 527 с. | 1 |
| 5 | Фороузан Б. А. Криптография и безопасность сетей : учебное пособие пер. с англ. Москва : ИНТУИТ : БИНОМ. Лаб. знаний : ЭКОМ, 2010. 783 с. 49 усл. печ. л. | 2 |
| 6 | 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 | Кульгин М. В. Практика построения компьютерных сетей. Санкт-Петербург [и др.] : Питер, 2001. 318 с. | 2 |
| 2 | Мак-Клар С., Скембрей Д., Курц Д. Секреты хакеров. Безопасность сетей - готовые решения : пер. с англ. 4-е изд. М. : Вильямс, 2004. 655 с. | 1 |
| 3 | Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учебное пособие для вузов. М. : Академия, 2006. 239 с. | 25 |
| 4 | Польман Н., Кразерс Т. Архитектура брандмауэров для сетей предприятия : пер. с англ. Москва : Вильямс, 2003. 420 с. | 1 |
| 5 | Устинов Г. Н. Основы информационной безопасности систем и сетей передачи данных : учебное пособие. Москва : СИНТЕГ, 2000. 235 с. | 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 | Безопасность вычислительных сетей | http://dgunh.ru/content/glavnay/ucheb_deyatel/uposob/up-it_ib-fgos-20.pdf | 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 |

### 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/ |
| 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 |

| Вид занятий | Наименование необходимого основного оборудования и технических средств обучения | Количество единиц |
|---|---|---|
| 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 «Безопасность вычислительных сетей»
***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 **Семестр**: 9,10

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

**Форма промежуточной аттестации:**
Экзамен: 9 семестр
Диф. зачет: 10 семестр

Пермь 2023

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

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

Согласно РПД, освоение учебного материала дисциплины запланировано в течение двух семестров (9-го, 10-го семестров учебного плана) и разбито на 6 учебных модулей. В каждом модуле предусмотрены аудиторные лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются компоненты компетенций **ОПК-10** и **ОПК-12,** сформулированных в компетентностной модели выпускника. З*нать, 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 заданиям 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** принципы построения и функционирования локальных и глобальных вычислительных сетей; последовательность и содержание этапов построения локальных вычислительных сетей; принципы построения и функционирования<br>**З.2 Знает** принципы организации и структуру систем защиты информации, основные протоколы, используемые для защиты информации в вычислительных сетях, основные криптографические методы, используемые для защиты информации в вычислительных сетях | | ТО1<br>ТО2<br>ТО3<br>ТО4 | | Т | | ТВ |
| **Освоенные умения** | | | | | | |
| **У.1 Умеет** использовать средства защиты информации вычислительных сетей<br>**У.2 Умеет** конфигурировать параметры системы защиты информации, контролировать эффективность принятых мер по реализации политик безопасности информации, проводить анализ угроз безопасности в локальных вычислительных сетях | | | ЛР 1<br>ЛР 2<br>ЛР 3<br>ЛР 4<br>ЛР 5<br>ЛР 6<br>ЛР 7 | Т | | ПЗ |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | ЛР 8<br>ЛР 9<br>ЛР 10 | | | |
| **Приобретенные владения** | | | | | | |
| **В.1 Владеет навыками** формирования модели угроз безопасности информации вычислительных сетей<br>**В.2 Владеет навыками** настройки сервисов безопасности в вычислительных сетях | | | ОЛР1<br>ПЗ 1<br>ПЗ 3<br>ПЗ 4 | Т | | 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, курсовая 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 учетом 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 в рамках контроля самостоятельной работы студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в журнал 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 отчета по результатам практических заданий (после изучения каждого модуля учебной дисциплины).

Всего запланировано 4 практических занятий. Темы практических занятий 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. Средства защиты. Основные направления защиты. Защита документов. Защита каналов утечки.
3. Мониторинг (аудит) действий пользователей.

4. Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные.
5. Нарушители, мотивированные извне. Другие типы нарушителей
6. Нетехнические меры защиты от внутренних угроз.
7. Психологические меры. Организационные меры.
8. Права локальных пользователей.
9. Стандартизация ПО. Специфические решения. Работа с кадрами. Хранение физических носителей.
10. Уровни контроля информационных потоков. Режим архива. Режим сигнализации. Режим активной защиты
11. Классификация firewall'ов. Установление TCP-соединения. Пакетные фильтры. Пограничные роутеры.
12. Пример набора правил пакетного фильтра. Stateful Inspection firewall'ы. Host-based firewall'ы. Персональные firewall'ы и персональные устройства firewall'а.
13. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Гибридные технологии firewall'а.
14. Информационная безопасность в проекции на семиуровневую модель ISO OSI
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. Идентификация и аутентификация как сервисы безопасности.
21. Управление доступом и его виды.
22. Авторизация как сервис безопасности.
23. Протоколирование и аудит как сервисы безопасности.
24. Криптографические сервисы безопасности.

**Типовые практические задания для контроля освоенных умений:**

1. Нетехнические меры защиты от внутренних угроз.
2. Классификация инструментальных средств анализа уязвимостей.
3. Типы компьютерных атак, обычно определяемые IDS.
4. Использование конфигурационных файлов веб-сервера Apache/NGINX для настройки прав доступа к каталогам.
5. Диагностирование работоспособности типовых сервисов инфо-коммуникационной инфраструктуры в ОС Windows, Linux.

### 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.