

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)



УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью

Сертификат: 1с6сfa0a-52a6-4f49-aef0-5584d3fd4820

Владелец: Троян Павел Ефимович

Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информационных процессов в сетях и системах связи

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки (специальность): **11.03.02 Инфокоммуникационные технологии и системы связи**

Направленность (профиль): **Защищенные системы и сети связи**

Форма обучения: **очная**

Факультет: **РТФ, Радиотехнический факультет**

Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**

Курс: **3**

Семестр: **6**

Учебный план набора 2016 года

Распределение рабочего времени

| № | Виды учебной деятельности | 6 семестр | Всего | Единицы |
|---|-----------------------------|-----------|-------|---------|
| 1 | Лекции | 34 | 34 | часов |
| 2 | Практические занятия | 38 | 38 | часов |
| 3 | Лабораторные работы | 36 | 36 | часов |
| 4 | Всего аудиторных занятий | 108 | 108 | часов |
| 5 | Самостоятельная работа | 72 | 72 | часов |
| 6 | Всего (без экзамена) | 180 | 180 | часов |
| 7 | Подготовка и сдача экзамена | 36 | 36 | часов |
| 8 | Общая трудоемкость | 216 | 216 | часов |
| | | 6.0 | 6.0 | З.Е |

Экзамен: 6 семестр

Томск 2017

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.03.02 Инфокоммуникационные технологии и системы связи, утвержденного 2015-03-06 года, рассмотрена и утверждена на заседании кафедры « ___ » _____ 20__ года, протокол № _____.

Разработчики:

доцент каф. РЗИ _____ Хатьков Н. Д.

Заведующий обеспечивающей каф.
РЗИ

_____ Задорин А. С.

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ Попова К. Ю.

Заведующий выпускающей каф.
РЗИ

_____ Задорин А. С.

Эксперты:

старший преподаватель каф. РЗИ _____ Зеленецкая Ю. В.

1. Цели и задачи дисциплины

1.1. Цели дисциплины

изучение способов защиты информационных процессов в сетях с гибридной физической средой

изучение возможностей применения стандартных настроек в сетях связи для повышения их защищенности

работа в компьютерных вычислительных сетях (ВС) с применением программных средств защиты и использования существующих, встроенных в архитектуру ОС, средств связи.

1.2. Задачи дисциплины

– изучение способов создания защищенного сетевого соединения, защищенных протоколов связи, защиты от несанкционированного доступа сообщений электронной почты, сетевых ресурсов

– изучение принципов работы брандмауэров, средств предотвращения вторжений, анти-вирусных программ

– развитие навыков настройки и анализа программных средств защиты, политик безопасности, использования программных отладчиков, сетевых анализаторов

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информационных процессов в сетях и системах связи» (Б1.В.ДВ.3.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Вычислительная техника и информационные технологии, Общая теория связи, Основы криптографии, Основы построения инфокоммуникационных систем и сетей.

Последующими дисциплинами являются: Комплексные системы защиты информации в сетях и системах связи, Организация и управление службой защиты информации на предприятиях связи, Сети связи и системы коммутации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-15 умением разрабатывать и оформлять различную проектную и техническую документацию;

– ПК-19 готовностью к организации работ по практическому использованию и внедрению результатов исследований;

В результате изучения дисциплины студент должен:

– **знать** основные подсистемы защиты средств связи в операционных системах персональных ЭВМ основы администрирования в ОС для контроля информационных процессов в компьютерных сетях методы и способы защиты от сетевых атак принципы построения систем обнаружения атак принципы защиты информации на компьютере средств связи с помощью программных реализаций на высоком и на низком уровне модели OSI

– **уметь** проводить анализ наличия несанкционированного доступа к компьютерам, определять и оценивать вероятные угрозы информационной безопасности компьютера в системах связи; осуществлять рациональный выбор средств и методов защиты информации на объектах связи;

– **владеть** программными методами защиты информации на компьютерной технике; методами поиска слабых мест в настройках компьютера и получения показателей уровня защищенности информации в системах связи; методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками настройки систем безопасности ОС для безопасной работы в сетях и системах связи;

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

| Виды учебной деятельности | Всего часов | Семестры |
|---------------------------|-------------|----------|
|---------------------------|-------------|----------|

| | | |
|---|-----|-----------|
| | | 6 семестр |
| Аудиторные занятия (всего) | 108 | 108 |
| Лекции | 34 | 34 |
| Практические занятия | 38 | 38 |
| Лабораторные работы | 36 | 36 |
| Самостоятельная работа (всего) | 72 | 72 |
| Оформление отчетов по лабораторным работам | 36 | 36 |
| Проработка лекционного материала | 10 | 10 |
| Подготовка к практическим занятиям, семинарам | 26 | 26 |
| Всего (без экзамена) | 180 | 180 |
| Подготовка и сдача экзамена | 36 | 36 |
| Общая трудоемкость ч | 216 | 216 |
| Зачетные Единицы | 6.0 | 6.0 |

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

| Названия разделов дисциплины | Лекции | Практические занятия | Лабораторные работы | Самостоятельная работа | Всего часов (без экзамена) | Формируемые компетенции |
|---|--------|----------------------|---------------------|------------------------|-------------------------------|-------------------------|
| 6 семестр | | | | | | |
| 1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions). | 2 | 4 | 4 | 7 | 17 | ПК-15, ПК-19 |
| 2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. | 2 | 4 | 4 | 7 | 17 | ПК-15, ПК-19 |
| 3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа. | 4 | 4 | 4 | 7 | 19 | ПК-15, ПК-19 |
| 4 Виды аудита компьютерных сетей и систем связи, классификация событий. | 4 | 4 | 8 | 11 | 27 | ПК-15, ПК-19 |
| 5 Программно-аппаратные средства | 4 | 4 | 4 | 7 | 19 | ПК-15, ПК-19 |

| | | | | | | |
|--|----|----|----|----|-----|--------------|
| шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами, логическая структура и компоненты PKI. | | | | | | |
| 6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. | 4 | 4 | 4 | 7 | 19 | ПК-15, ПК-19 |
| 7 Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт. | 4 | 4 | 4 | 7 | 19 | ПК-15, ПК-19 |
| 8 Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID. | 4 | 4 | 0 | 5 | 13 | ПК-15, ПК-19 |
| 9 Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы как особый класс РПВ. | 4 | 4 | 4 | 9 | 21 | ПК-15, ПК-19 |
| 10 Защита от разрушающих программных воздействий (РПВ) в компьютерных системах связи. | 2 | 2 | 0 | 5 | 9 | ПК-15, ПК-19 |
| Итого за семестр | 34 | 38 | 36 | 72 | 180 | |
| Итого | 34 | 38 | 36 | 72 | 180 | |

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

| Названия разделов | Содержание разделов дисциплины по лекциям | Трудоемкость, ч | Формируемые компетенции |
|--|---|-----------------|-------------------------|
| 6 семестр | | | |
| 1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоя в оперативной памяти, общие принципы построения систем защиты (triple functions). | Предмет и задачи защиты информационных процессов в сетях и системах связи, ее взаимосвязь с другими дисциплинами. Краткая история развития. Актуальность защиты информации в современном мире. Причины возникновения уязвимостей, общие принципы построения систем защиты (triple functions). Понятие политики безопасности и необходимости оценки рисков, критерии, используемые для | 2 | ПК-15, ПК-19 |

| | | | |
|---|---|---|--------------|
| | классификации уровня защищенности (безопасности) компьютерных сетей и системы связи. | | |
| | Итого | 2 | |
| 2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. | Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. Методы аутентификации: парольная схема, биометрический и token способы, многофакторная и взаимная аутентификации. Протоколы идентификации с нулевой передачей знаний. Схемы идентификации Фейге-Фиата-Шамира, Гиллоу-Куискуотера. | 2 | ПК-15, ПК-19 |
| | Итого | 2 | |
| 3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа. | Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам. Дискреционная (разграничительная) модель управления доступом. Анализ систем дискреционного разграничения доступа на основе формальной модели Take-Grant. Доступ к данным со стороны процесса. Способы фиксации факта доступа. Надежность систем ограничения доступа. Управление доступом на основе ролей – RBAC. Базовая модель RBAC. Мандатная (представительная) модель управления доступом. Механизмы реализации мандатной модели доступа. Защита файлов от изменения. Субъект и диспетчер допуска, особенности реализации. Средства управления доступом, используемые в современных операционных системах. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 4 Виды аудита компьютерных сетей и систем связи, классификация событий. | Виды аудита, классификация событий. Контроль целостности данных, использование цифровой подписи. Средства аудита, реализованные в современных сетях и системах связи. Системы предотвращения и обнаружения вторжений, локальные и беспроводные - IPS IDS HIPS WIPS. | 4 | ПК-15, ПК-19 |

| | | | |
|--|---|---|--------------|
| | Итого | 4 | |
| 5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами, логическая структура и компоненты РКІ. | Генерация ключей. Ключи для симметричных и несимметричных алгоритмов. Обмен ключами, алгоритм Диффи-Хеллмана. Эфемерный ключ. Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами, логическая структура и компоненты РКІ. Угрозы криптографическим ключам. Усечение ключевого множества. Повреждение ключей. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты систем связи. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. | Классификация методов защиты информационных процессов в сетях и системах связи. Методы и средства ограничения доступа к компонентам ЭВМ, защиты программ от несанкционированного копирования. Программные и технические средства защиты. Защита программ от излучения. Устаревшие технические средства защиты. Защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям. Применение обфускации, протекторов и упаковщиков для усиления защиты системы связи. Методы, затрудняющие считывание скопированной информации. Пароли и ключи, организация хранения ключей. Методы, препятствующие использованию скопированной информации. Основные функции средств защиты от копирования. Приемы противодействия динамическим способам снятия защиты программ от копирования. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 7 Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт. | Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт. Контактные и бесконтактные смарт – карты с соответствующими интерфейсами ISO – 7816, USB (RuToken, eToken), ISO/ IEC 14443.. | 4 | ПК-15, ПК-19 |

| | | | |
|--|---|----|--------------|
| | Интеллектуальные карты. Жизненный цикл смарт-карт. Выпускаемые серийно интегральные схемы смарт-карт. Инфраструктура поддержки смарт-карт. Проблемы безопасности смарт-карт. Классификация атак на смарт-карты. | | |
| | Итого | 4 | |
| 8 Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID. | Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID. Передача данных в системах RFID, способы кодирования. Считыватели и транспондеры, электронные компоненты систем RFID, стандартизация. Обеспечение безопасности данных. Примеры применения: идентификация товаров, транспортных средств, иммобилайзерные системы, идентификация животных. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 9 Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы как особый класс РПВ. | Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы, как особый класс РПВ. Развитие вирусной базы и тенденции формирования новых типов вирусов. Способы заражения локальных компьютеров и сетей. Программные черви и закладки. Необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды. Средства противодействия компьютерным вирусам и их состояние в современных условиях. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 10 Защита от разрушающих программных воздействий (РПВ) в компьютерных системах связи. | Защита от разрушающих программных воздействий (РПВ). Проблема восстановления операционной системы после воздействия РПВ и применения средств противодействия в системах связи. | 2 | ПК-15, ПК-19 |
| | Итого | 2 | |
| Итого за семестр | | 34 | |

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

| Наименование дисциплин | № разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин | | | | | | | | | |
|--|---|---|---|---|---|---|---|---|---|----|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Предшествующие дисциплины | | | | | | | | | | |
| 1 Вычислительная техника и информационные технологии | + | | + | | + | | | | | |
| 2 Общая теория связи | | | | + | | | | + | | |
| 3 Основы криптографии | | | | | + | | | | | |
| 4 Основы построения инфокоммуникационных систем и сетей | + | | | + | | | | | | + |
| Последующие дисциплины | | | | | | | | | | |
| 1 Комплексные системы защиты информации в сетях и системах связи | | + | | + | + | | | | | + |
| 2 Организация и управление службой защиты информации на предприятиях связи | | | | | | + | | | + | |
| 3 Сети связи и системы коммутации | | | | | | | + | + | + | |

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

| Компетенции | Виды занятий | | | | Формы контроля |
|-------------|--------------|----------------------|---------------------|------------------------|--|
| | Лекции | Практические занятия | Лабораторные работы | Самостоятельная работа | |
| ПК-15 | + | + | + | + | Экзамен, Конспект самоподготовки, Отчет по лабораторной работе, Опрос на занятиях, Отчет по практике |
| ПК-19 | + | + | + | + | Экзамен, Конспект самоподготовки, Отчет по лабораторной работе, Опрос на занятиях, Отчет по практике |

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

| Названия разделов | Наименование лабораторных работ | Трудоемкость, ч | Формируемые компетенции |
|---|--|--------------------|----------------------------|
| 6 семестр | | | |
| 1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions). | Анализ процессов в операционной системе Windows с помощью подготовленной утилиты. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. | Исследование парольной защиты компонент связи на основе дизассемблирования трех видов тестовых утилит с парольной защитой и скрытой формой представления интерфейсных компонент. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа. | Анализ совмещенных систем защиты доступа в одной и той же ОС. Анализ возможностей поисковых серверов в области технической IP адресации (поиск адресов веб камер, сетевого и другого оборудования). | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 4 Виды аудита компьютерных сетей и систем связи, классификация событий. | Утилиты Марка Руссиновича для мониторинга ОС Windows. Мониторинг состояния операционной системы с помощью утилиты arimonitor-x86. | 4 | ПК-15, ПК-19 |
| | Сетевые анализаторы трафика - снифферы. On-line и локальный снифферы. Установка, настройка фильтров, выделение потока с данными. Декодирование выделенных пакетов трафика на примере передачи изображений. | 4 | |
| | Итого | 8 | |
| 5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления | Использование шифрованной файловой системы (EFS). Создание разделов, под разделов с помощью проводника Windows. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |

| | | | |
|--|---|----|-----------------|
| сертификатами, логическая структура и компоненты PKI. | | | |
| 6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. | Изучение способа предотвращения выполнения данных с помощью встроенных средств ОС. Предотвращение выполнения данных (Data Execution Prevention, DEP) — с помощью функции безопасности, встроенной в Linux, Mac OS X, Android и Windows. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 7 Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт. | Токены. Многофакторная аутентификация. Способы установки и виды доступа в систему связи. Применение Dallas - Lock. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 9 Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы как особый класс РПВ. | Исследование вируса. Способы исследования. Выявление предположительной страны изготовления и функций, сопутствующих его работе в информационных процессах. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| Итого за семестр | | 36 | |

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

| Названия разделов | Наименование практических занятий (семинаров) | Трудоемкость, ч | Формируемые компетенции |
|---|---|-----------------|-------------------------|
| 6 семестр | | | |
| 1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions). | Карта информационного процесса в оперативной памяти ОС. Наличие адресов физических носителей информации. Возможность переполнения памяти и воздействие этого явления на информационный процесс. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. | Методы входа в сетевые сервера различного типа: почтовый, файловый, веб-сервер, сервер баз данных, коммуникационный сервер связи, сервер - принтер и виртуальные сервера. Общие и частные проблемы идентификации и аутентификации серверов. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 3 Классификация субъектов и | Абстрактные модели доступа, история | 4 | ПК-15, |

| | | | |
|--|---|---|--------------|
| объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа. | развития. Основные идеи и свойства объектов и субъектов в моделях доступа. Логические построения и комбинации моделей доступа в системах связи.. | | ПК-19 |
| | Итого | 4 | |
| 4 Виды аудита компьютерных сетей и систем связи, классификация событий. | Аудит компьютерных сетей. Внутренний и внешний аудит. Ручной, полуавтоматический и автоматический аудит компьютерных сетей. Основные политики настроек в программном обеспечении, возможность проверок на нижнем уровне модели OSI. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами, логическая структура и компоненты PKI. | Программно-аппаратные средства шифрования - основные параметры. Открытый доступ к ресурсам и вопросы его защиты в системе связи. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. | Средства ограничения доступа к системам связи. Основные меры защиты оперативной памяти коммуникационных устройств. Особенности защиты процессов записи и воспроизведения информации. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 7 Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт. | Строение простой смарт-карты. Виды доступа к информационным процессам смарт-карт в том числе с помощью удаленных устройств связи. Возможности программирования смарт-карт. Запись и считывание данных с смарт-карт. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 8 Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID. | Радиочастотная идентификация, как один из вариантов удаленных средств доступа к объектам связи. Организация периметральной защиты объектов связи на основе транспондеров и интеррогаторов. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 9 Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы как особый класс РПВ. | Описание типов вирусов. Основной механизм распространения. Базовые принципы поиска вирусов в антивирусных программах. Способы безопасного анализа вирусов. Наличие виру- | 4 | ПК-15, ПК-19 |

| | | | |
|---|---|----|--------------|
| | сов в системах связи. | | |
| | Итого | 4 | |
| 10 Защита от разрушающих программных воздействий (РПВ) в компьютерных системах связи. | Lock блокираторы функций записи-чтения в ОС. UnLock деблокиатор связанных программ. Принцип работы и использования. | 2 | ПК-15, ПК-19 |
| | Итого | 2 | |
| Итого за семестр | | 38 | |

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|---|---|-----------------|-------------------------|---|
| 6 семестр | | | | |
| 1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоя в оперативной памяти, общие принципы построения систем защиты (triple functions). | Подготовка к практическим занятиям, семинарам | 2 | ПК-15, ПК-19 | Опрос на занятиях, Отчет по лабораторной работе, Отчет по практике |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 7 | | |
| 2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. | Подготовка к практическим занятиям, семинарам | 2 | ПК-15, ПК-19 | Конспект самоподготовки, Отчет по лабораторной работе, Отчет по практике, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 7 | | |
| 3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа. | Подготовка к практическим занятиям, семинарам | 2 | ПК-15, ПК-19 | Конспект самоподготовки, Отчет по лабораторной работе, Отчет по практике, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 7 | | |
| 4 Виды аудита компьютерных сетей и | Подготовка к практическим занятиям, семинарам | 2 | ПК-15, ПК-19 | Конспект самоподготовки, Отчет по лабораторной работе, Отчет по практике, Экзамен |

| | | | | |
|--|---|----|-----------------|--|
| систем связи, классификация событий. | рам | | | ной работе, Отчет по практике, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 11 | | |
| 5 Программно- аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами, логическая структура и компоненты PKI. | Подготовка к практиче- ским занятиям, семина- рам | 2 | ПК-15, ПК-19 | Конспект самоподготов- ки, Отчет по лаборатор- ной работе, Отчет по практике, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 7 | | |
| 6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. | Подготовка к практиче- ским занятиям, семина- рам | 2 | ПК-15, ПК-19 | Конспект самоподготов- ки, Отчет по лаборатор- ной работе, Отчет по практике, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 7 | | |
| 7 Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт- карт. | Подготовка к практиче- ским занятиям, семина- рам | 2 | ПК-15, ПК-19 | Конспект самоподготов- ки, Отчет по лаборатор- ной работе, Отчет по практике, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 7 | | |
| 8 Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID. | Подготовка к практиче- ским занятиям, семина- рам | 4 | ПК-15, ПК-19 | Конспект самоподготов- ки, Отчет по практике, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 5 | | |

| | | | | |
|--|---|-----|--------------|---|
| 9 Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы как особый класс РПВ. | Подготовка к практическим занятиям, семинарам | 4 | ПК-15, ПК-19 | Конспект самоподготовки, Отчет по лабораторной работе, Отчет по практике, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 9 | | |
| 10 Защита от разрушающих программных воздействий (РПВ) в компьютерных системах связи. | Подготовка к практическим занятиям, семинарам | 4 | ПК-15, ПК-19 | Конспект самоподготовки, Отчет по практике, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 5 | | |
| Итого за семестр | | 72 | | |
| | Подготовка и сдача экзамена | 36 | | Экзамен |
| Итого | | 108 | | |

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

| Элементы учебной деятельности | Максимальный балл на 1-ую КТ с начала семестра | Максимальный балл за период между 1КТ и 2КТ | Максимальный балл за период между 2КТ и на конец семестра | Всего за семестр |
|-------------------------------|--|---|---|------------------|
| 6 семестр | | | | |
| Конспект самоподготовки | 3 | 3 | 4 | 10 |
| Опрос на занятиях | 5 | 5 | 6 | 16 |
| Отчет по лабораторной работе | 5 | 5 | 6 | 16 |
| Отчет по практике | 9 | 9 | 10 | 28 |
| Итого максимум за период | 22 | 22 | 26 | 70 |
| Экзамен | | | | 30 |
| Нарастающим итогом | 22 | 44 | 70 | 100 |

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

| Баллы на дату контрольной точки | Оценка |
|---|--------|
| ≥ 90% от максимальной суммы баллов на дату КТ | 5 |
| От 70% до 89% от максимальной суммы баллов на дату КТ | 4 |

| | |
|---|---|
| От 60% до 69% от максимальной суммы баллов на дату КТ | 3 |
| < 60% от максимальной суммы баллов на дату КТ | 2 |

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка (ГОС) | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS) |
|--------------------------------------|--|-------------------------|
| 5 (отлично) (зачтено) | 90 - 100 | A (отлично) |
| 4 (хорошо) (зачтено) | 85 - 89 | B (очень хорошо) |
| | 75 - 84 | C (хорошо) |
| | 70 - 74 | D (удовлетворительно) |
| 65 - 69 | | |
| 3 (удовлетворительно) (зачтено) | 60 - 64 | E (посредственно) |
| 2 (неудовлетворительно) (не зачтено) | Ниже 60 баллов | F (неудовлетворительно) |

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Системы контроля и управления доступом. (Серия «Обеспечение безопасности объектов»; Выпуск 2). / В.А. Ворона, В.А. Тихонов. — М. : Горячая линия-Телеком, 2013. — 272 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5135>
2. Системы и сети связи. Демидов, А.Я.— уч. пособие — М. : ТУСУР, 2012. — 61 с. [Электронный ресурс]. - <http://e.lanbook.com/book/11030>
3. Защита информационных процессов в компьютерных системах: Учебное пособие / Пушкарев В. В., Пушкарев В. П. - 2012. 131 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1507>, дата обращения: 08.02.2017.

12.2. Дополнительная литература

1. Комплексные (интегрированные) системы обеспечения безопасности. (Серия «Обеспечение безопасности объектов»; Выпуск 7). / В.А. Ворона, В.А. Тихонов.— М. : Горячая линия-Телеком, 2013. — 160 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5136>
2. Операционные системы. Концепции построения и обеспечения безопасности. / Ю.Ф. Мартемьянов, А.В. Яковлев, А.В. Яковлев. — М. : Горячая линия-Телеком, 2011. — 332 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5176>
3. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова. — М. : Горячая линия-Телеком, 2012. — 550 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5114>

12.3. Литература для практических занятий.

1. Сети связи и системы коммутации: Руководство к практическим занятиям / Винокуров В. М. - 2012. 41 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1517>, дата обращения: 08.02.2017.

12.4. Литература для самостоятельной работы.

1. Методы моделирования и оптимизации телекоммуникационных систем и сетей: Учебно-методическое пособие к практическим занятиям и самостоятельной работы / Демидов А. Я. - 2012. 55 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2840>, дата обращения: 08.02.2017.

2. Локальные компьютерные сети: Методические указания по самостоятельной работе / Агеев Е. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2037>, дата обращения: 08.02.2017.

12.5 Учебно-методические пособия

12.5.1. Обязательные учебно-методические пособия

1. Основы построения коммутационных полей систем коммутации (ОПКПСК): Руководство к лабораторным занятиям и самостоятельной работе студентов / Винокуров В. М. - 2012. 115 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2500>, дата обращения: 08.02.2017.

2. Программирование: Методические рекомендации к лабораторным работам / Титков А. В. - 2011. 13 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/661>, дата обращения: 08.02.2017.

3. Использование сетевых программных утилит Windows: Методические указания к лабораторным работам / Агеев Е. Ю. - 2012. 17 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2041>, дата обращения: 08.02.2017.

4. Изучение сетевого протокола TCP/IP: Методические указания к лабораторным работам / Агеев Е. Ю. - 2012. 16 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2040>, дата обращения: 08.02.2017.

12.5.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.6. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. <http://www.rambler.ru/>
2. <http://www.sputnik.ru/>
3. <https://www.yandex.ru/>

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется 412 учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины для демонстрации на компьютерном проекторе, установленном в аудитории.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебная аудитория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 74, 4 этаж, ауд. 412. Состав оборудования: Учебная мебель; Доска магнитно-маркерная -1шт.; Коммутатор D-Link Switch 24 port - 1шт.; Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. -14 шт. Ис-

пользуется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3/Microsoft Windows 7 Professional with SP1; Microsoft Windows Server 2008 R2; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft Office Access 2003; VirtualBox 6.2. Имеется помещения для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 74, 4 этаж, ауд. 412. Состав оборудования: Учебная мебель; Экран с электроприводом DRAPER BARONET – 1 шт.; Мультимедийный проектор TOSHIBA – 1 шт.; Компьютеры класса не ниже Intel Pentium G3220 (3.0GHz/4Mb)/4GB RAM/ 500GB с широкополосным доступом в Internet, с мониторами типа Samsung 18.5" S19C200N– 18 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft SQL-Server 2005; Matlab v6.5

13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 1 этаж, ауд. 126. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

| Категории студентов | Виды дополнительных оценочных средств | Формы контроля и оценки результатов обучения |
|---|---|--|
| С нарушениями слуха | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы | Преимущественно письменная проверка |
| С нарушениями зрения | Собеседование по вопросам к зачету, опрос по терминам | Преимущественно устная проверка (индивидуально) |
| С нарушениями опорно-двигательного аппарата | Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету | Преимущественно дистанционными методами |
| С ограничениями по общемедицинским показаниям | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы | Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки |

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)**

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«__» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Защита информационных процессов в сетях и системах связи

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки (специальность): **11.03.02 Инфокоммуникационные технологии и системы связи**

Направленность (профиль): **Защищенные системы и сети связи**

Форма обучения: **очная**

Факультет: **РТФ, Радиотехнический факультет**

Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**

Курс: **3**

Семестр: **6**

Учебный план набора 2016 года

Разработчики:

– доцент каф. РЗИ Хатьков Н. Д.

Экзамен: 6 семестр

Томск 2017

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

| Код | Формулировка компетенции | Этапы формирования компетенций |
|-------|---|---|
| ПК-15 | умением разрабатывать и оформлять различную проектную и техническую документацию | <p>Должен знать основные подсистемы защиты средств связи в операционных системах персональных ЭВМ основы администрирования в ОС для контроля информационных процессов в компьютерных сетях методы и способы защиты от сетевых атак принципы построения систем обнаружения атак принципы защиты информации на компьютере средств связи с помощью программных реализаций на высоком и на низком уровне модели OSI;</p> <p>Должен уметь проводить анализ наличия несанкционированного доступа к компьютерам, определять и оценивать вероятные угрозы информационной безопасности компьютера в системах связи; осуществлять рациональный выбор средств и методов защиты информации на объектах связи;;</p> <p>Должен владеть программными методами защиты информации на компьютерной технике; методами поиска слабых мест в настройках компьютера и получения показателей уровня защищенности информации в системах связи; методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками настройки систем безопасности ОС для безопасной работы в сетях и системах связи;;</p> |
| ПК-19 | готовностью к организации работ по практическому использованию и внедрению результатов исследований | |

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

| Показатели и критерии | Знать | Уметь | Владеть |
|---------------------------|---|---|--|
| Отлично (высокий уровень) | Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости | Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем | Контролирует работу, проводит оценку, совершенствует действия работы |
| Хорошо (базовый) | Знает факты, принципы, | Обладает диапазоном | Берет ответственность за |

| | | | |
|---------------------------------------|--|--|---|
| уровень) | процессы, общие понятия в пределах изучаемой области | практических умений, требуемых для решения определенных проблем в области исследования | завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем |
| Удовлетворительно (пороговый уровень) | Обладает базовыми общими знаниями | Обладает основными умениями, требуемыми для выполнения простых задач | Работает при прямом наблюдении |

2 Реализация компетенций

2.1 Компетенция ПК-15

ПК-15: умением разрабатывать и оформлять различную проектную и техническую документацию.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|----------------------------------|---|---|--|
| Содержание этапов | Методики сбора и анализа информации для проектирования аппаратных средств и сетей связи и их элементов на основе приложений в области телекоммуникаций. | Осуществлять поиск и анализ информации в области защиты систем связи, представленной в различных отечественных и зарубежных источниках для проектирования средств и сетей связи. | Навыками расчетов различных конфигураций сетей, проектированием топологии сетей, необходимых при анализе информации для проектирования средств и сетей связи и их элементов. |
| Виды занятий | <ul style="list-style-type: none"> • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; | <ul style="list-style-type: none"> • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; | <ul style="list-style-type: none"> • Лабораторные работы; • Самостоятельная работа; |
| Используемые средства оценивания | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Опрос на занятиях; • Конспект самоподготовки; • Отчет по практике; • Экзамен; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Опрос на занятиях; • Конспект самоподготовки; • Отчет по практике; • Экзамен; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Отчет по практике; • Экзамен; |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---------------------------|--|--|--|
| Отлично (высокий уровень) | <ul style="list-style-type: none"> • Знает основные тенденции развития сетей и систем связи; Анализирует на основе информационного поиска | <ul style="list-style-type: none"> • Умеет грамотно проводить анализ технической информации; Умеет применять знания для решения различных | <ul style="list-style-type: none"> • Свободно владеет разными способами представления информации; Владеет расчетами параметров компо- |

| | | | |
|---------------------------------------|--|--|---|
| | связи между различными компонентами ее аппаратной реализации и понятиями в этой области; Знает основные возможности поисковых систем для реализации конкурентно-способных технических решений. ; | задач распространения информации в сетях и системах связи. ; | ентов устройств связи. Владеет методами решения задач анализа топологий сетей и систем связи. ; |
| Хорошо (базовый уровень) | <ul style="list-style-type: none"> Понимает соотношения между различными понятиями в области связи; Представляет приемы и результаты анализа технической информации.; | <ul style="list-style-type: none"> Умеет осуществлять поиск информации в области сетей и систем связи, представленной в различных отечественных и зарубежных источниках; Умеет самостоятельно подбирать методы решения задач в области связи. ; | <ul style="list-style-type: none"> Владеет навыками работы с литературными источниками связанными с распространением информации в сетях и системах связи.; |
| Удовлетворительно (пороговый уровень) | <ul style="list-style-type: none"> Воспроизводит основные положения анализа технической информации; Дает определения основных понятий в области связи. ; | <ul style="list-style-type: none"> Умеет работать со справочной литературой; умеет представлять результаты своей работы. ; | <ul style="list-style-type: none"> Способен корректно представить знания и информацию связанную с сетевыми топологиями на основе компьютерных сетей и их компонентов.; |

2.2 Компетенция ПК-19

ПК-19: готовностью к организации работ по практическому использованию и внедрению результатов исследований.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|-------------------|---|---|---|
| Содержание этапов | Должен знать принципы построения сетей и систем связи; основы защиты информации при передаче информации по различным типам линий связи, основные методы расчета параметров компонентов устройств связи, анализ и мониторинг сетей связи от внешних и внутренних вредных воздействий; основные положения по проектированию линий связи; классификацию и типы вирусных про- | Должен уметь применять на практике политику настроек ПО сетей и систем связи различного назначения; осуществлять грамотный выбор вида безопасной передачи информационных сообщений в зависимости от внутренних и внешних условий вредных воздействий; осуществлять грамотный выбор технологии и методов использования антивирусного ПО на различных этапах формирова- | Должен владеть навыками формирования топологий сетей связи, их адресации на основе применения современных коммуникационных компонентов сетей; навыками проектирования защиты информационных процессов для линий связи, прокладываемых на сетях различного назначения; навыками работы с антивирусными программами и средствами мониторинга сетей связи, а также набором |

| | | | |
|----------------------------------|---|--|--|
| | грамм: настройки политики безопасности антивирусного ПО; основы защиты информационных процессов в сетях связи и повышения их надежности. | ния сетей связи; применять на практике эффективные методы настройки политики безопасности линий связи и определения места и характера возникновения вредоносных воздействий; определять на основе мониторинга сетей основные показатели их защищенности; | свойств настроек политики безопасности сетей связи; навыками работы с оборудованием, использующем средства аутентификации и идентификации; |
| Виды занятий | <ul style="list-style-type: none"> • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; | <ul style="list-style-type: none"> • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа; | <ul style="list-style-type: none"> • Лабораторные работы; • Самостоятельная работа; |
| Используемые средства оценивания | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Опрос на занятиях; • Конспект самоподготовки; • Отчет по практике; • Экзамен; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Опрос на занятиях; • Конспект самоподготовки; • Отчет по практике; • Экзамен; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Отчет по практике; • Экзамен; |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---------------------------|---|---|--|
| Отлично (высокий уровень) | <ul style="list-style-type: none"> • Знает основные тенденции развития инфокоммуникационных технологий и систем связи в области использования защиты информационных процессов; Анализирует связи между различными понятиями в области построения защиты коммуникационного и др. оборудования. Знает основные параметры, используемые в связи для минимизации скорости передачи информации при ее кодировании, методы их решения. ; | <ul style="list-style-type: none"> • Умеет грамотно проводить анализ технической информации; Умеет применять знания для решения различных связанных задач по защите информации.; | <ul style="list-style-type: none"> • Свободно владеет разными способами представления информации; Владеет методами решения связанных задач в области защиты информационных процессов. ; |
| Хорошо (базовый) | <ul style="list-style-type: none"> • Понимает связи меж- | <ul style="list-style-type: none"> • Умеет осуществлять | <ul style="list-style-type: none"> • Владеет навыками ра- |

| | | | |
|---------------------------------------|---|---|---|
| уровень) | ду различными понятиями в области защиты информационных процессов в сетях связи; Представляет приемы и результаты анализа технической информации в различных топологиях линий связи.; | поиск информации в области связи для защиты информационных процессов, представленной в различных отечественных и зарубежных источниках; Умеет самостоятельно подбирать методы решения проблем в области безопасности систем связи.; | боты с литературными источниками связанными с анализом защищенности информационных процессов в системах связи.; |
| Удовлетворительно (пороговый уровень) | <ul style="list-style-type: none"> • Воспроизводит основные положения анализа технической информации по вредоносным воздействиям на компоненты линий связи; Дает определения основных понятий в области линий связи по проведению технических мероприятий, связанных с защитой информационных процессов. ; | <ul style="list-style-type: none"> • Умеет работать со справочной литературой; умеет представлять результаты своей работы. ; | <ul style="list-style-type: none"> • Способен корректно представить знания и информацию, связанную с информационными процессами в системах связи.; |

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Вопросы на самоподготовку

– Способы предотвращения выполнения данных с помощью встроенных средств ОС. Изучить Data Execution Prevention, DEP — функции безопасности, встроенной в Linux, Mac OS X, Android и Windows. Получить информацию по токенам в проблеме многофакторной аутентификации. Определить способы установки и виды доступа в систему связи. Провести анализ совмещенных систем защиты доступа в одной и той же ОС на примере Windows. Осуществить анализ возможностей поисковых серверов в области технической IP адресации для сетевого и другого оборудования. Получить последние новости по работе вирусов в мировой практике, новые способы исследования. Привести материалы по повышению устойчивости парольной защиты компонент связи к сетевым атакам.

3.2 Темы опросов на занятиях

– Архитектура встроенных средств защиты в ОС. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. Основные подходы к защите данных от НСД. Абстрактные модели доступа. Виды аудита компьютерных сетей и систем связи. Построение аппаратных компонент криптозащиты данных. Управления открытыми ключами. Методы защиты программ. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях. Защита программ от несанкционированного копирования. Аппаратные компоненты смарт-карт и программное обеспечение для смарт-карт. Базовые принципы радиочастотной идентификации. Сетевые вирусы как особый класс РПВ.

3.3 Экзаменационные вопросы

– Представить карту информационного процесса в оперативной памяти ОС. Указать на-

личные адреса физических носителей информации. Оценить возможность переполнения памяти и воздействие этого явления на информационный процесс. Представить методы входа в сетевые сервера различного типа: почтовый, файловый, веб-сервер, сервер баз данных, коммуникационный сервер связи, сервер - принтер и виртуальные сервера. Определить общие и частные проблемы идентификации и аутентификации серверов. Представить абстрактные модели доступа, история развития. Указать основные идеи и свойства объектов и субъектов в моделях доступа. Составить логические построения и комбинации моделей доступа в системах связи. Назначение аудита компьютерных сетей. Цели внутреннего и внешнего аудита сетей связи. Описать ручной, полуавтоматический и автоматический аудит компьютерных сетей. Представить основные политики настроек в программном обеспечении, возможность проверок на нижнем уровне модели OSI. Указать основные параметры программно-аппаратных средств шифрования. Пояснить для чего существует открытый доступ к ресурсам и как организовать его защиту в системе связи. Назвать средства ограничения доступа к системам связи. Привести основные меры защиты оперативной памяти коммуникационных устройств. Представить особенности защиты процессов записи и воспроизведения информации. Представить строение простой смарт-карты. Указать виды доступа к информационным процессам смарт-карт в том числе с помощью удаленных устройств связи. Назвать типовые возможности программирования смарт-карт. Пояснить процессы записи и считывания данных с смарт-карт. Показать, что радиочастотная идентификация является одним из вариантов удаленных средств доступа к объектам связи. Представить организацию периметральной защиты объектов связи на основе транспондеров и интеррогаторов. Дать описание типов вирусов. Указать основной механизм распространения. Показать базовые принципы поиска вирусов в антивирусных программах. Представить способы безопасного анализа вирусов. Показать, как определяется наличие вирусов в системах связи. Что такое Lock блокираторы функций записи-чтения в ОС. Для чего необходим UnLock деблокиатор связанных программ. Указать принцип работы и использования блокираторов программ.

3.4 Вопросы для подготовки к практическим занятиям, семинарам

- Карта информационного процесса в оперативной памяти ОС. Наличие адресов физических носителей информации. Возможность переполнения памяти и воздействие этого явления на информационный процесс.
- Методы входа в сетевые сервера различного типа: почтовый, файловый, веб-сервер, сервер баз данных, коммуникационный сервер связи, сервер - принтер и виртуальные сервера. Общие и частные проблемы идентификации и аутентификации серверов.
- Абстрактные модели доступа, история развития. Основные идеи и свойства объектов и субъектов в моделях доступа. Логические построения и комбинации моделей доступа в системах связи..
- Аудит компьютерных сетей. Внутренний и внешний аудит. Ручной, полуавтоматический и автоматический аудит компьютерных сетей. Основные политики настроек в программном обеспечении, возможность проверок на нижнем уровне модели OSI.
- Программно-аппаратные средства шифрования - основные параметры. Открытый доступ к ресурсам и вопросы его защиты в системе связи.
- Средства ограничения доступа к системам связи. Основные меры защиты оперативной памяти коммуникационных устройств. Особенности защиты процессов записи и воспроизведения информации.
- Строение простой смарт-карты. Виды доступа к информационным процессам смарт-карт в том числе с помощью удаленных устройств связи. Возможности программирования смарт-карт. Запись и считывание данных с смарт-карт.
- Радиочастотная идентификация, как один из вариантов удаленных средств доступа к объектам связи. Организация периметральной защиты объектов связи на основе транспондеров и интеррогаторов.
- Описание типов вирусов. Основной механизм распространения. Базовые принципы поиска вирусов в антивирусных программах. Способы безопасного анализа вирусов. Наличие вирусов в системах связи.
- Lock блокираторы функций записи-чтения в ОС. UnLock деблокиатор связанных про-

грамм. Принцип работы и использования.

3.5 Темы лабораторных работ

- Анализ процессов в операционной системе Windows с помощью подготовленной утилиты.
- Утилиты Марка Руссиновича для мониторинга ОС Windows. Мониторинг состояния операционной системы с помощью утилиты arimonitor-x86.
- Использование шифрованной файловой системы (EFS). Создание разделов, под разделов с помощью проводника Windows.
- Сетевые анализаторы трафика - снифферы. On-line и локальный снифферы. Установка, настройка фильтров, выделение потока с данными. Декодирование выделенных пакетов трафика на примере передачи изображений.
- Изучение способа предотвращения выполнения данных с помощью встроенных средств ОС. Предотвращение выполнения данных (Data Execution Prevention, DEP) — с помощью функции безопасности, встроенной в Linux, Mac OS X, Android и Windows.
- Токены. Многофакторная аутентификация. Способы установки и виды доступа в систему связи. Применение Dallas - Lock.
- Анализ совмещенных систем защиты доступа в одной и той же ОС. Анализ возможностей поисковых серверов в области технической IP адресации (поиск адресов веб камер, сетевого и другого оборудования).
- Исследование вируса. Способы исследования. Выявление предположительной страны изготовления и функций, сопутствующих его работе в информационных процессах.
- Исследование парольной защиты компонент связи на основе дизассемблирования трех видов тестовых утилит с парольной защитой и скрытой формой представления интерфейсных компонент.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Системы контроля и управления доступом. (Серия «Обеспечение безопасности объектов»; Выпуск 2). / В.А. Ворона, В.А. Тихонов. — М. : Горячая линия-Телеком, 2013. — 272 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5135>
2. Системы и сети связи. Демидов, А.Я.— уч. пособие — М. : ТУСУР, 2012. — 61 с. [Электронный ресурс]. - <http://e.lanbook.com/book/11030>
3. Защита информационных процессов в компьютерных системах: Учебное пособие / Пушкарев В. В., Пушкарев В. П. - 2012. 131 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1507>, дата обращения: 08.02.2017.

4.2. Дополнительная литература

1. Комплексные (интегрированные) системы обеспечения безопасности. (Серия «Обеспечение безопасности объектов»; Выпуск 7). / В.А. Ворона, В.А. Тихонов.— М. : Горячая линия-Телеком, 2013. — 160 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5136>
2. Операционные системы. Концепции построения и обеспечения безопасности. / Ю.Ф. Мартемьянов, А.В. Яковлев, А.В. Яковлев. — М. : Горячая линия-Телеком, 2011. — 332 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5176>
3. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова. — М. : Горячая линия-Телеком, 2012. — 550 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5114>

4.3. Литература для практических занятий.

1. Сети связи и системы коммутации: Руководство к практическим занятиям / Винокуров В. М. - 2012. 41 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1517>, дата обращения: 08.02.2017.

4.4. Литература для самостоятельной работы.

1. Методы моделирования и оптимизации телекоммуникационных систем и сетей: Учебно-методическое пособие к практическим занятиям и самостоятельной работы / Демидов А. Я. - 2012. 55 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2840>, дата обращения: 08.02.2017.

2. Локальные компьютерные сети: Методические указания по самостоятельной работе / Агеев Е. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2037>, дата обращения: 08.02.2017.

4.5 Учебно-методические пособия

4.5.1. Обязательные учебно-методические пособия

1. Основы построения коммутационных полей систем коммутации (ОПКПСК): Руководство к лабораторным занятиям и самостоятельной работе студентов / Винокуров В. М. - 2012. 115 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2500>, дата обращения: 08.02.2017.

2. Программирование: Методические рекомендации к лабораторным работам / Титков А. В. - 2011. 13 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/661>, дата обращения: 08.02.2017.

3. Использование сетевых программных утилит Windows: Методические указания к лабораторным работам / Агеев Е. Ю. - 2012. 17 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2041>, дата обращения: 08.02.2017.

4. Изучение сетевого протокола TCP/IP: Методические указания к лабораторным работам / Агеев Е. Ю. - 2012. 16 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2040>, дата обращения: 08.02.2017.

4.6. Базы данных, информационно справочные и поисковые системы

1. <http://www.rambler.ru/>
2. <http://www.sputnik.ru/>
3. <https://www.yandex.ru/>