

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)



УТВЕРЖДАЮ

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 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: **4**

Семестр: **7**

Учебный план набора 2014 года

Распределение рабочего времени

| № | Виды учебной деятельности | 7 семестр | Всего | Единицы |
|---|---------------------------|-----------|-------|---------|
| 1 | Лекции | 24 | 24 | часов |
| 2 | Практические занятия | 18 | 18 | часов |
| 3 | Лабораторные работы | 18 | 18 | часов |
| 4 | Всего аудиторных занятий | 60 | 60 | часов |
| 5 | Самостоятельная работа | 48 | 48 | часов |
| 6 | Всего (без экзамена) | 108 | 108 | часов |
| 7 | Общая трудоемкость | 108 | 108 | часов |
| | | 3.0 | 3.0 | З.Е |

Зачет: 7 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 06 марта 2015 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол № _____.

Разработчики:

доцент каф. РЗИ

_____ Н. Д. Хатьков

Заведующий обеспечивающей каф.
РЗИ

_____ А. С. Задорин

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

Декан РТФ

_____ К. Ю. Попова

Заведующий выпускающей каф.
РЗИ

_____ А. С. Задорин

Эксперты:

старший преподаватель каф. РЗИ

_____ Ю. В. Зеленецкая

1. Цели и задачи дисциплины

1.1. Цели дисциплины

изучение способов защиты информационных процессов в сетях с гибридной физической средой

изучение возможностей применения программно-аппаратных средств 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, антивирусных программ на основе использования средств защиты информационных процессов

– 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 системах связи» (Б1.В.ДВ.9.1) относится к блоку 1 (вариативная часть).

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

Последующими дисциплинами являются: Информационные технологии, Сети и системы цифровой радиосвязи и радиодоступа.

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 программно-аппаратных систем обнаружения атак, принципы защиты информации на компьютере средств связи с помощью программных реализаций на высоком и на низком уровне

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

– **владеть** методами защиты информации на компьютерной технике в процессах записи, хранения и копирования, 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 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

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

| | | |
|---|-----|-----------|
| | | 7 семестр |
| Аудиторные занятия (всего) | 60 | 60 |
| Лекции | 24 | 24 |
| Практические занятия | 18 | 18 |
| Лабораторные работы | 18 | 18 |
| Самостоятельная работа (всего) | 48 | 48 |
| Оформление отчетов по лабораторным работам | 18 | 18 |
| Проработка лекционного материала | 12 | 12 |
| Подготовка к практическим занятиям, семинарам | 18 | 18 |
| Всего (без экзамена) | 108 | 108 |
| Общая трудоемкость ч | 108 | 108 |
| Зачетные Единицы | 3.0 | 3.0 |

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 |
|---|--------|----------------------|---------------------|------------------------|-------------------------------|-------------------------|
| 7 семестр | | | | | | |
| 1 Информационные процессы в системах связи, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям связи. Общие принципы построения систем защиты информационных процессов. | 2 | 4 | 0 | 6 | 12 | ПК-15, ПК-19 |
| 2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. | 4 | 0 | 4 | 5 | 13 | ПК-15, ПК-19 |
| 3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД в системах связи. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информа- | 2 | 2 | 0 | 3 | 7 | ПК-15, ПК-19 |

| | | | | | | |
|---|----|----|----|----|-----|--------------|
| ции. | | | | | | |
| 4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита. | 2 | 0 | 6 | 7 | 15 | ПК-15, ПК-19 |
| 5 Организация защищенного процесса шифрования. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами. | 2 | 4 | 0 | 6 | 12 | ПК-15, ПК-19 |
| 6 Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. | 2 | 0 | 0 | 1 | 3 | ПК-15, ПК-19 |
| 7 Защита информационных процессов на основе надстроек над операционной системой. Многофакторная система аутентификации. | 4 | 4 | 0 | 5 | 13 | ПК-15, ПК-19 |
| 8 Разрушающие программные воздействия (РПВ). Классификация РПВ. Признаки наличия РПВ в информационных процессах. Возможности анализа разрушающих воздействий на ПО. | 2 | 0 | 0 | 1 | 3 | ПК-15, ПК-19 |
| 9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ. | 2 | 0 | 4 | 5 | 11 | ПК-15, ПК-19 |
| 10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI. | 2 | 4 | 4 | 9 | 19 | ПК-15, ПК-19 |
| Итого за семестр | 24 | 18 | 18 | 48 | 108 | |
| Итого | 24 | 18 | 18 | 48 | 108 | |

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 |
|---|---|-----------------|-------------------------|
| 7 семестр | | | |
| 1 Информационные процессы в системах связи, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям связи. | Предмет и задачи защиты информационных процессов в системах связи, ее взаимосвязь с другими дисциплинами. Краткая история развития. Актуальность защиты информационных про- | 2 | ПК-15, ПК-19 |

| | | | |
|---|--|---|--------------|
| Общие принципы построения систем защиты информационных процессов. | цессов в современном мире. Состав информационных процессов. Причины возникновения уязвимостей, общие принципы построения систем защиты информационных процессов. Понятие политики безопасности и необходимости оценки рисков, критерии, используемые для классификации уровня защищенности (безопасности) систем связи. | | |
| | Итого | 2 | |
| 2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. | Основные понятия, классификация задач, решаемых информационными процессами. Проблемы идентификации субъекта, понятие протокола идентификации, идентифицирующая информация в информационном процессе. 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 и основные проблемы их реализации. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД в системах связи. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации. | Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа. Шифрование в информационном процессе, контроль доступа и разграничение доступа. Иерархический принцип доступа к файлу. Программная фиксация доступа к файлам. Дискреционная (разграничительная) модель управления доступом на основе формальной модели Take-Grant и проблемы ее реализации. Способы фиксации факта доступа. Надежность систем ограничения доступа. Управление доступом на основе ролей – RBAC. Базовая модель RBAC. Мандатная (представительная) модель управления доступом. Программная реализации мандатной модели доступа. | 2 | ПК-15, ПК-19 |
| | Итого | 2 | |
| 4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита. | Виды аудита компьютерных систем связи. Контроль целостности данных. Программные системы предотвращения и обнаружения вторжений, локальные и беспроводные - IPS IDS HIPS WIPS. | 2 | ПК-15, ПК-19 |

| | | | |
|---|--|---|-----------------|
| | Итого | 2 | |
| 5 Организация защищенного процесса шифрования. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами. | Генерация ключей программно-аппаратными средствами. Ключи для симметричных и несимметричных алгоритмов. Эфемерный ключ. Информационные процессы с компонентами криптозащиты данных. Угрозы криптографическим ключам. Повреждение ключей. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции средства криптозащиты систем связи. | 2 | ПК-15, ПК-19 |
| | Итого | 2 | |
| 6 Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. | Средства ограничения доступа к компонентам информационного процесса в системах связи. Встроенная программная защита от изучения информационных процессов в системах связи. Устаревшие технические средства защиты. Программная защита от отладки, защита от дизассемблирования, защита от трассировки по аппаратным прерываниям процессорных процедур. Применение обфускации, протекторов и упаковщиков для усиления защиты системы связи. Методы, затрудняющие считывание скопированной информации. Основные функции средств защиты от копирования. | 2 | ПК-15, ПК-19 |
| | Итого | 2 | |
| 7 Защита информационных процессов на основе надстроек над операционной системой. Многофакторная система аутентификации. | Программные надстройки над ОС для защиты информационных процессов. Противоречия программных настроек и встроенных систем защиты информационных процессов в ОС. Получение многофакторная аутентификации за счет программных надстроек над операционной системой. Токены. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 8 Разрушающие программные воздействия (РПВ). Классификация РПВ. Признаки наличия РПВ в информационных процессах. Возможности анализа разрушающих воздействий на ПО. | Компьютерные вирусы, как особый класс разрушающих программных воздействий. Развитие вирусной базы и тенденции формирования новых типов вирусов. Программные черви и закладки. | 2 | ПК-15, ПК-19 |
| | Итого | 2 | |
| 9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных | Средства противодействия компьютерным вирусам и их состояние в современных условиях. Маскировка вирус- | 2 | ПК-15, ПК-19 |

| | | | |
|--|---|----|-----------------|
| системах связи. Недостатки антивирусных программ. | ных программ. Способы проникновения вирусов в информационные процессы системы связи. Проблемы минимизации последствий деятельности вирусов после их удаления из системы связи. | | |
| | Итого | 2 | |
| 10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI. | Принципиальная возможность перехвата трафика в системах связи. Снифферы - назначение, состав и принцип работы. Настройки фильтров и уровни работы в информационном процессе. Возможности анализа сегментов трафика и его перехвата. Изучение свойств информационного процесса в системе связи с помощью сниффера. | 2 | ПК-15, ПК-19 |
| | Итого | 2 | |
| Итого за семестр | | 24 | |

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 | + | | + | | + | | | | | |
| 2 Общая теория связи | | | | + | | | + | | + | |
| 3 Основы криптографии | | | | | + | | | | | |
| 4 Основы построения инфокоммуникационных систем и сетей | | | | | | + | | | | + |
| Последующие дисциплины | | | | | | | | | | |
| 1 Информационные технологии | + | + | | | | | | | | + |
| 2 Сети и системы цифровой радиосвязи и радиодоступа | | | | | | + | | + | + | |

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 | + | + | + | + | Отчет по лабораторной работе, Зачет, Отчет по практическому занятию |
| ПК-19 | + | + | + | + | Отчет по лабораторной работе, Зачет, Отчет по практическому занятию |

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 |
|---|---|-----------------|-------------------------|
| 7 семестр | | | |
| 2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. | Исследование парольной защиты компонент связи на основе использования дизассемблеров в ручном, полуавтоматическом и автоматическом режимах. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита. | Программы для ручного, полуавтоматического и автоматического аудита компьютерных сетей. Исследование состояния компьютерной сети и настройка соответствующих политик аудита этих сетей. | 4 | ПК-15, ПК-19 |
| | Маршрутизаторы. Состав, назначения свойства. Работа маршрутизатора в имитационном режиме. Удаленная настройка доступа в сеть. Основные команды. | 2 | |

| | | | |
|--|--|----|-----------------|
| | Итого | 6 | |
| 9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ. | Исследование доступа к компьютерной системе связи с помощью тестовых утилит. Определение возможности внешнего управления интерфейсом сторонних программ. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI. | Wireshark – анализатор сетевых протоколов, фиксация потоков в сети связи в интерактивном режиме, просмотр содержания сетевых фреймов. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| Итого за семестр | | 18 | |

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 |
|--|--|-----------------|-------------------------|
| 7 семестр | | | |
| 1 Информационные процессы в системах связи, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям связи. Общие принципы построения систем защиты информационных процессов. | Наличие адресов физических носителей информации. Карта и структура оперативной памяти компьютера. Возможность аппаратного влияния на процессы обмена информацией в оперативной памяти компьютера. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД в системах связи. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации. | Абстрактные модели доступа, история развития. Основные аппаратные идеи для реализации моделей доступа. Общие требования к логическим построениям в программном обеспечении при реализации различных моделей доступа. | 2 | ПК-15, ПК-19 |
| | Итого | 2 | |
| 5 Организация защищенного процесса шифрования. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами. | Программная реализация проводника в Windows и других файловых менеджеров для шифрования доступа к файлам на локальной компьютерной системе. Общие требования к службам Windows для обеспечения их безопасного использования для защиты данных. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| 7 Защита информационных | Надстройки операционной системы. | 4 | ПК-15, |

| | | | |
|--|---|----|-----------------|
| процессов на основе надстроек над операционной системой. Многофакторная система аутентификации. | Отечественная система Dallas Lock 8.0 к - состав, назначение, способ установки, организация многофакторной защиты. | | ПК-19 |
| | Итого | 4 | |
| 10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI. | Работа сниффера в системах связи. Настройка фильтров для выявления паролей. Определение уровня работы в модели OSI. | 4 | ПК-15, ПК-19 |
| | Итого | 4 | |
| Итого за семестр | | 18 | |

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 |
|---|---|-----------------|-------------------------|---------------------------------------|
| 7 семестр | | | | |
| 1 Информационные процессы в системах связи, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям связи. Общие принципы построения систем защиты информационных процессов. | Подготовка к практическим занятиям, семинарам | 4 | ПК-15, ПК-19 | Зачет, Отчет по практическому занятию |
| | Проработка лекционного материала | 2 | | |
| | Итого | 6 | | |
| 2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. | Проработка лекционного материала | 1 | ПК-15, ПК-19 | Зачет, Отчет по лабораторной работе |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 5 | | |
| 3 Классификация | Подготовка к практическим занятиям, семинарам | 2 | ПК-15, | Зачет, Отчет по практическому занятию |

| | | | | |
|--|---|---|-----------------|---------------------------------------|
| субъектов и объектов доступа. Основные подходы к защите данных от НСД в системах связи. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации. | ским занятиям, семинарам | | ПК-19 | ческому занятию |
| | Проработка лекционного материала | 1 | | |
| | Итого | 3 | | |
| 4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита. | Проработка лекционного материала | 1 | ПК-15, ПК-19 | Зачет, Отчет по лабораторной работе |
| | Оформление отчетов по лабораторным работам | 6 | | |
| | Итого | 7 | | |
| 5 Организация защищенного процесса шифрования. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами. | Подготовка к практическим занятиям, семинарам | 4 | ПК-15, ПК-19 | Зачет, Отчет по практическому занятию |
| | Проработка лекционного материала | 2 | | |
| | Итого | 6 | | |
| 6 Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования. | Проработка лекционного материала | 1 | ПК-15, ПК-19 | Зачет |
| | Итого | 1 | | |
| 7 Защита информационных процессов на основе надстроек над операционной системой. Многофакторная система аутентификации. | Подготовка к практическим занятиям, семинарам | 4 | ПК-15, ПК-19 | Зачет, Отчет по практическому занятию |
| | Проработка лекционного материала | 1 | | |
| | Итого | 5 | | |
| 8 Разрушающие программные воздействия (РПВ). Классификация РПВ. Признаки наличия РПВ в информационных процессах. Возможности анализа разрушающих | Проработка лекционного материала | 1 | ПК-15, ПК-19 | Зачет |
| | Итого | 1 | | |

| | | | | |
|--|---|----|--------------|---|
| воздействий на ПО. | | | | |
| 9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ. | Проработка лекционного материала | 1 | ПК-15, ПК-19 | Зачет, Отчет по лабораторной работе |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 5 | | |
| 10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI. | Подготовка к практическим занятиям, семинарам | 4 | ПК-15, ПК-19 | Зачет, Отчет по лабораторной работе, Отчет по практическому занятию |
| | Проработка лекционного материала | 1 | | |
| | Оформление отчетов по лабораторным работам | 4 | | |
| | Итого | 9 | | |
| Итого за семестр | | 48 | | |
| Итого | | 48 | | |

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 |
|--------------------------------|--|---|---|------------------|
| 7 семестр | | | | |
| Зачет | 7 | 8 | 15 | 30 |
| Отчет по лабораторной работе | 10 | 15 | 15 | 40 |
| Отчет по практическому занятию | 10 | 10 | 10 | 30 |
| Итого максимум за период | 27 | 33 | 40 | 100 |
| Нарастающим итогом | 27 | 60 | 100 | 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. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2012. — 320 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5150>
4. 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: 17.03.2017.

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>

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: 17.03.2017.

12.4. Литература для самостоятельной работы.

1. Основы компьютерных сетевых технологий: Методические рекомендации к организации самостоятельной работы / Агеев Е. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1657>, дата обращения: 17.03.2017.

12.5 Учебно-методические пособия

12.5.1. Обязательные учебно-методические пособия

1. Методы шифрования информации: Методические указания к лабораторным работам / Агеев Е. Ю. - 2012. 15 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2039>, дата обращения: 17.03.2017.
2. 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: 17.03.2017.

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 учебная аудитория 418, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

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. Используется 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 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: **4**

Семестр: **7**

Учебный план набора 2014 года

Разработчики:

– доцент каф. РЗИ Н. Д. Хатьков

Зачет: 7 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 программно-аппаратных систем обнаружения атак, принципы защиты информации на компьютере средств связи с помощью программных реализаций на высоком и на низком уровне;</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 программно-аппаратных средств и методов защиты информации на объектах связи;</p> <p>Должен владеть методами защиты информации на компьютерной технике в процессах записи, хранения и копирования, 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 уровень) | Знает факты, принципы, процессы, общие понятия в пределах изучаемой области | Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования | Берет ответственность за 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 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; • Отчет по практическому занятию; • Зачет; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Отчет по практическому занятию; • Зачет; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Отчет по практическому занятию; • Зачет; |

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 связи между различными | <ul style="list-style-type: none"> • Умеет грамотно проводить анализ технической информации; Умеет применять знания для решения различных задач распространения | <ul style="list-style-type: none"> • Свободно владеет разными способами представления информации; Владеет расчетами параметров компонентов устройств связи. |

| | | | |
|---------------------------------------|--|---|---|
| | ми компонентами ее аппаратурной реализации и понятиями в этой области; Знает основные возможности поисковых систем для реализации конкурентно-способных технических решений.; | информации в сетях и системах 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 программ: настройки поли- | 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 формирования сетей связи; приме- | 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 свойств настроек поли- |

| | | | |
|----------------------------------|---|--|--|
| | тики безопасности анти-вирусного ПО; основы защиты информационных процессов в сетях связи и повышения их надежности. | нять 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. | тики 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; • Отчет по практическому занятию; • Зачет; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Отчет по практическому занятию; • Зачет; | <ul style="list-style-type: none"> • Отчет по лабораторной работе; • Отчет по практическому занятию; • Зачет; |

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 уровень) | <ul style="list-style-type: none"> • Понимает связи между различными понятиями в области защиты информационных про- | <ul style="list-style-type: none"> • Умеет осуществлять поиск информации в области связи для защиты информационных | <ul style="list-style-type: none"> • Владеет навыками работы с литературными источниками связанными с анализом защи- |

| | | | |
|--|--|---|---|
| | <p>цессов в сетях связи; Представляет приемы и результаты анализа технической информации в различных топологиях линий связи.;</p> | <p>процессов, представленной в различных отечественных и зарубежных источниках; Умеет самостоятельно подбирать методы решения проблем в области безопасности систем связи.;</p> | <p>ценности информационных процессов в системах связи.;</p> |
| <p>Удовлетворительно (пороговый уровень)</p> | <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 Зачёт

– Представить карту информационного процесса в оперативной памяти ОС. Указать наличие адресов 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 деблокиратор связанных программ. Указать принцип работы и использования блокираторов программ.

3.2 Вопросы для подготовки к практическим занятиям, семинарам

- Наличие адресов физических носителей информации. Карта и структура оперативной памяти компьютера. Возможность аппаратного влияния на процессы обмена информацией в оперативной памяти компьютера.
- Абстрактные модели доступа, история развития. Основные аппаратные идеи для реализации моделей доступа. Общие требования к логическим построениям в программном обеспечении при реализации различных моделей доступа.
- Программная реализация проводника в Windows и других файловых менеджеров для шифрования доступа к файлам на локальной компьютерной системе. Общие требования к службам Windows для обеспечения их безопасного использования для защиты данных.
- Настройки операционной системы. Отечественная система Dallas Lock 8.0 к - состав, назначение, способ установки, организация многофакторной защиты.
- Работа сниффера в системах связи. Настройка фильтров для выявления паролей. Определение уровня работы в модели OSI.

3.3 Темы лабораторных работ

- Исследование парольной защиты компонент связи на основе использования дизассемблеров в ручном, полуавтоматическом и автоматическом режимах.
- Программы для ручного, полуавтоматического и автоматического аудита компьютерных сетей. Исследование состояния компьютерной сети и настройка соответствующих политик аудита этих сетей.
- Исследование доступа к компьютерной системе связи с помощью тестовых утилит. Определение возможности внешнего управления интерфейсом сторонних программ.
- Wireshark – анализатор сетевых протоколов, фиксация потоков в сети связи в интерактивном режиме, просмотр содержания сетевых фреймов.
- Маршрутизаторы. Состав, назначения свойства. Работа маршрутизатора в имитационном режиме. Удаленная настройка доступа в сеть. Основные команды.

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. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2012. — 320 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5150>
4. 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>, свободный.

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. [Элек-

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: 17.03.2017.

4.4. Литература для самостоятельной работы.

1. Основы компьютерных сетевых технологий: Методические рекомендации к организации самостоятельной работы / Агеев Е. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1657>, дата обращения: 17.03.2017.

4.5. Обязательные учебно-методические пособия

1. Методы шифрования информации: Методические указания к лабораторным работам / Агеев Е. Ю. - 2012. 15 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2039>, свободный.

2. 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>, свободный.

4.6. Базы данных, информационно справочные и поисковые системы

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