**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.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

# Управление средствами защиты информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль): **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **3, 4**
Семестр: **6, 7**
Учебный план набора 2014 года

Распределение рабочего времени

| № | Виды учебной деятельности | 6 семестр | 7 семестр | Всего | Единицы |
|---|---|---|---|---|---|
| 1 | Лекции | 18 | | 18 | часов |
| 2 | Практические занятия | | 8 | 8 | часов |
| 3 | Лабораторные работы | 28 | | 28 | часов |
| 4 | Контроль самостоятельной работы (курсовой проект / курсовая работа) | | 28 | 28 | часов |
| 5 | Всего аудиторных занятий | 46 | 36 | 82 | часов |
| 6 | Из них в интерактивной форме | 14 | 2 | 16 | часов |
| 7 | Самостоятельная работа | 26 | 36 | 62 | часов |
| 8 | Всего (без экзамена) | 72 | 72 | 144 | часов |
| 9 | Общая трудоемкость | 72 | 72 | 144 | часов |
| | | 2.0 | 2.0 | 4.0 | З.Е |

Зачет: 6 семестр
Курсовая работа (проект): 7 семестр

Согласована на портале № 13641

Рассмотрена и одобрена на заседании кафедры
протокол № 2 от «12» 2 2017 г.

Томск 2017

Согласована на портале № 13641

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 2016-11-16 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

Ассистент каф. БИС _____ Рахманенко И. А.

Заведующий обеспечивающей каф. КИБЭВС _____ Шелупанов А. А.

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

Декан ФБ _____ Давыдова Е. М.

Заведующий выпускающей каф. БИС _____ Мещеряков Р. В.

Эксперты:

доцент каф. КИБЭВС _____ Конев А. А.

Согласована на портале № 13641

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью преподавания дисциплины является освоение методов управления программными средствами защиты информации, реализованными на основе клиент-серверной технологии.

### 1.2. Задачи дисциплины

– Получение знаний о методах контроля работоспособности и целостности клиентских модулей средств защиты информации;

– Получение знаний о методах сбора и отображения серверным модулем журналов аудита клиентских модулей;

– Получение умений и навыков централизованного управления клиентскими модулями и реагирования на угрозы безопасности.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Управление средствами защиты информации» (Б1.В.ОД.10) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Администрирование сетей ЭВМ, Безопасность операционных систем.

Последующими дисциплинами являются: Распределенные автоматизированные информационные системы.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-14 способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем;

В результате изучения дисциплины студент должен:

– **знать** принципы организации информационных систем в соответствии с требованиями по защите информации.

– **уметь** эффективно использовать различные методы и средства защиты информации для компьютерных сетей; администрировать подсистемы информационной безопасности автоматизированных систем.

– **владеть** навыками выявления и уничтожения компьютерных вирусов; методами и средствами выявления угроз безопасности автоматизированным системам.

## 4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

| Виды учебной деятельности | Всего часов | Семестры | |
|---|---|---|---|
| | | 6 семестр | 7 семестр |
| Аудиторные занятия (всего) | 82 | 46 | 36 |
| Лекции | 18 | 18 | |
| Практические занятия | 8 | | 8 |
| Лабораторные работы | 28 | 28 | |
| Контроль самостоятельной работы (курсовой проект / курсовая работа) | 28 | | 28 |
| Из них в интерактивной форме | 16 | 14 | 2 |
| Самостоятельная работа (всего) | 62 | 26 | 36 |
| Выполнение курсового проекта (работы) | 36 | | 36 |

Согласована на портале № 13641

| | | | |
|---|---|---|---|
| Оформление отчетов по лабораторным работам | 22 | 22 | |
| Проработка лекционного материала | 4 | 4 | |
| Всего (без экзамена) | 144 | 72 | 72 |
| Общая трудоемкость ч | 144 | 72 | 72 |
| Зачетные Единицы | 4.0 | 2.0 | 2.0 |

## 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 | Курсовая работа | Всего часов (без экзамена) | Формируемые компетенции |
|---|---|---|---|---|---|---|---|
| 6 семестр | | | | | | | |
| 1 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях. | 4 | 0 | 4 | 4 | 0 | 12 | ПК-14 |
| 2 Централизованная защита от вирусов в локальной сети. | 4 | 0 | 4 | 4 | 0 | 12 | ПК-14 |
| 3 Централизованное управление средствами защиты от несанкционированного доступа в локальной сети. | 4 | 0 | 16 | 14 | 0 | 34 | ПК-14 |
| 4 Централизованный учет и управление программно-аппаратными средствами защиты информации. | 6 | 0 | 4 | 4 | 0 | 14 | ПК-14 |
| Итого за семестр | 18 | 0 | 28 | 26 | 0 | 72 | |
| 7 семестр | | | | | | | |
| 5 Администрирование и управление средствами защиты информации от несанкционированного доступа. | 0 | 8 | 0 | 36 | 28 | 44 | ПК-14 |
| Итого за семестр | 0 | 8 | 0 | 36 | 28 | 72 | |
| Итого | 18 | 8 | 28 | 62 | 28 | 144 | |

Согласована на портале № 13641

### 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 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях. | Знакомство с интерфейсом «КБ Инвентаризация»; подготовка к инспекциям; инспекции компьютеров; получение отчетов с результатами инспектирования. Удалённый контроль работоспособности средств защиты информации на рабочих станциях. | 4 | ПК-14 |
| | Итого | 4 | |
| 2 Централизованная защита от вирусов в локальной сети. | Управление серверами администрирования; управление группами администрирования; управление клиентскими компьютерами; работа с отчетами, статистикой. | 4 | ПК-14 |
| | Итого | 4 | |
| 3 Централизованное управление средствами защиты от несанкционированного доступа в локальной сети. | Принципы построения СЗИ “Secret Net”; основные механизмы защиты; аппаратные средства; конфигурирование; аудит; мониторинг и оперативное управление; полномочное управление доступом и контроль печати. | 4 | ПК-14 |
| | Итого | 4 | |
| 4 Централизованный учет и управление программно-аппаратными средствами защиты информации. | Назначение «SafeNet Authentication Manager»; возможности; архитектура; настройка; управление жизненным циклом средств аутентификации; аудит использования средств аутентификации. | 6 | ПК-14 |
| | Итого | 6 | |
| Итого за семестр | | 18 | |
| Итого | | 18 | |

### 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.

Согласована на портале № 13641

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 |
| Предшествующие дисциплины | | | | | |
| 1 Администрирование сетей ЭВМ | + | + | + | | + |
| 2 Безопасность операционных систем | + | | + | + | + |
| Последующие дисциплины | | | | | |
| 1 Распределенные автоматизированные информационные системы | | | + | + | |

**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 | Контроль самостоятельной работы (курсовой проект / курсовая работа) | Самостоятельная работа | |

Согласована на портале № 13641

| | | | | | | |
|---|---|---|---|---|---|---|
| ПК-14 | + | + | + | + | + | Конспект самоподготовки, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов (работ), Зачет |

## 6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

| Методы | Интерактивные лабораторные занятия | Интерактивные лекции | Интерактивные практические занятия | Всего |
|---|---|---|---|---|
| 6 семестр | | | | |
| Презентации с использованием слайдов с обсуждением | | 6 | | 6 |
| Case-study (метод конкретных ситуаций) | 4 | | | 4 |
| Решение ситуационных задач | 4 | | | 4 |
| Итого за семестр: | 8 | 6 | 0 | 14 |
| 7 семестр | | | | |
| Решение ситуационных задач | | | 2 | 2 |
| Итого за семестр: | 0 | 0 | 2 | 2 |
| Итого | 8 | 6 | 2 | 16 |

## 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 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях. | “КБ Инвентаризация”. Проведение инспекций | 4 | ПК-14 |
| | Итого | 4 | |
| 2 Централизованная защита от | Управление серверами | 4 | ПК-14 |

Согласована на портале № 13641

| | | | |
|---|---|---|---|
| вирусов в локальной сети. | администрирования KSC | | |
| | Итого | 4 | |
| 3 Централизованное управление средствами защиты от несанкционированного доступа в локальной сети. | Аутентификация в операционной системе. Разграничение доступа к данным | 4 | ПК-14 |
| | Разграничение доступа к устройствам. Замкнутая программная среда. Контроль целостности | 4 | |
| | Работа со сведениями в журнале регистрации событий. Теневое копирование | 4 | |
| | Secret Net. Оперативное управление | 4 | |
| | Итого | 16 | |
| 4 Централизованный учет и управление программно-аппаратными средствами защиты информации. | Управление жизненным циклом средств аутентификации | 4 | ПК-14 |
| | Итого | 4 | |
| Итого за семестр | | 28 | |
| Итого | | 28 | |

## 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 | | | |
| 5 Администрирование и управление средствами защиты информации от несанкционированного доступа. | Администрирование и управление СЗИ от НСД Secret Net | 8 | ПК-14 |
| | Итого | 8 | |
| Итого за семестр | | 8 | |
| Итого | | 8 | |

## 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 Централизованная инвентаризация | Проработка лекционного материала | 1 | ПК-14 | Зачет, Защита отчета, Конспект |

Согласована на портале № 13641

| | | | | |
|---|---|---|---|---|
| ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях. | Оформление отчетов по лабораторным работам | 3 | | самоподготовки, Опрос на занятиях, Отчет по лабораторной работе |
| | Итого | 4 | | |
| 2 Централизованная защита от вирусов в локальной сети. | Проработка лекционного материала | 1 | ПК-14 | Зачет, Защита отчета, Конспект самоподготовки, Отчет по лабораторной работе |
| | Оформление отчетов по лабораторным работам | 3 | | |
| | Итого | 4 | | |
| 3 Централизованное управление средствами защиты от несанкционированного доступа в локальной сети. | Проработка лекционного материала | 1 | ПК-14 | Зачет, Защита отчета, Конспект самоподготовки, Отчет по лабораторной работе |
| | Оформление отчетов по лабораторным работам | 13 | | |
| | Итого | 14 | | |
| 4 Централизованный учет и управление программно-аппаратными средствами защиты информации. | Проработка лекционного материала | 1 | ПК-14 | Зачет, Защита отчета, Конспект самоподготовки, Отчет по лабораторной работе |
| | Оформление отчетов по лабораторным работам | 3 | | |
| | Итого | 4 | | |
| Итого за семестр | | 26 | | |
| 7 семестр | | | | |
| 5 Администрирование и управление средствами защиты информации от несанкционированного доступа. | Выполнение курсового проекта (работы) | 36 | ПК-14 | Защита курсовых проектов (работ) |
| | Итого | 36 | | |
| Итого за семестр | | 36 | | |
| Итого | | 62 | | |

### 9.1. Темы курсовых проектов (работ)

1. Администрирование и управление СЗИ от НСД Secret Net

## 10. Курсовая работа (проект)

Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсовой работы (проекта) представлены таблице 10.1.

Таблица 10. 1 – Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсовой работы (проекта)

| Наименование аудиторных занятий | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|
| 7 семестр | | |
| Основной темой курсовых работ по дисциплине “Управление средствами защиты информации” является тема | 28 | ПК-14 |

Согласована на портале № 13641

| | | |
|---|---|---|
| “Администрирование и управление СЗИ от НСД Secret Net”. Совместно с руководителем возможен выбор другой темы курсовой работы, однако необходимым является условие применения в рамках курсовой работы средства защиты от несанкционированного доступа в локальной сети с применением выданных преподавателем виртуальных машин. | | |
| Итого за семестр | 28 | |

### 10.1 Темы курсовых работ

Примерная тематика курсовых работ (проектов):

– Разработка и управление средствами защиты автоматизированных систем. Курсовая работа выполняется по вариантам.

## 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 | | | | |
| Зачет | | | 20 | 20 |
| Защита отчета | 15 | 15 | 15 | 45 |
| Конспект самоподготовки | | 5 | 5 | 10 |
| Опрос на занятиях | | 5 | 5 | 10 |
| Отчет по лабораторной работе | 5 | 5 | 5 | 15 |
| Итого максимум за период | 20 | 30 | 50 | 100 |
| Нарастающим итогом | 20 | 50 | 100 | 100 |
| 7 семестр | | | | |
| Защита курсовых проектов (работ) | | | 100 | 100 |
| Итого максимум за период | | | 100 | 100 |
| Нарастающим итогом | 0 | 0 | 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 |

Согласована на портале № 13641

### 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) |
| 3 (удовлетворительно) (зачтено) | 65 - 69 | |
| | 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. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 4-е изд., стер. - М. : Академия, 2009. - 336 с. : ил., табл. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. (наличие в библиотеке ТУСУР - 21 экз.)

### 12.2. Дополнительная литература

1. Компьютерные сети: Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2013. - 944 с. : ил., табл. - (Учебник для вузов. Стандарт третьего поколения). (наличие в библиотеке ТУСУР - 20 экз.)
2. Защита информации с использованием смарт-карт и электронных брелоков / Л. К. Бабенко, С. С. Ищуков, О. Б. Макаревич. - М. : "Гелиос АРВ", 2003. - 351[1] с. : ил., табл., портр. - Библиогр.: с. 348-349. (наличие в библиотеке ТУСУР - 30 экз.)

### 12.3 Учебно-методические пособия

#### 12.3.1. Обязательные учебно-методические пособия

1. Рахманенко И.А. Методические указания по выполнению практических работ по дисциплине Управление средствами защиты информации [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_pract.pdf
2. Рахманенко И.А. Лабораторный практикум по дисциплине “Управление средствами защиты информации” [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_lab.pdf
3. Рахманенко И.А. Методические указания для выполнения курсовой работы по дисциплине Управление средствами защиты информации [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_course.pdf
4. Рахманенко И.А. Методические указания для выполнения самостоятельной и индивидуальной работы по дисциплине Управление средствами защиты информации [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_sam.pdf

#### 12.3.2 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;

Согласована на портале № 13641

– 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.

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

1. Система подготовки документов Open Office; Система для использования виртуальных машин VMware Player; Google; Wikipedia.

## 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 лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 3 этаж, ауд. 310. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор ViewSonic PJD5151 – 1 шт.; Компьютер лекционный acer travelmate 2300; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2, Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

#### 13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 404. Состав оборудования: Учебная мебель; TraceBoard TS-408L - 1 шт.; Мультимедийный проектор Benq – 1 шт.; Компьютеры класса не ниже Celeron 2.4 GHz/256Mb/40Gb с широкополосным доступом в Internet, – 4 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2; Имеется помещение 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 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 402. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Мультимедийный проектор Benq – 1 шт.; Компьютеры класса не ниже AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb. с широкополосным доступом в Internet, – 15 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

#### 13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для проведения самостоятельной работы используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 402. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Мультимедийный проектор Benq – 1 шт.; Компьютеры класса не ниже AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb. с широкополосным доступом в Internet, – 15 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения

Согласована на портале № 13641

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

Согласована на портале № 13641

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.

Согласована на портале № 13641

**Приложение 1**

**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

# Управление средствами защиты информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль): **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **3, 4**
Семестр: **6, 7**

Учебный план набора 2014 года

Разработчики:

- Ассистент каф. БИС Рахманенко И. А.

Зачет: 6 семестр
Курсовая работа (проект): 7 семестр

Томск 2017

Согласована на портале № 13641

## 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-14 | способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем | Должен знать принципы организации информационных систем в соответствии с требованиями по защите информации.; Должен уметь эффективно использовать различные методы и средства защиты информации для компьютерных сетей; администрировать подсистемы информационной безопасности автоматизированных систем. ; Должен владеть навыками выявления и уничтожения компьютерных вирусов; методами и средствами выявления угроз безопасности автоматизированным системам. ; |

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-14

ПК-14: способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и

Согласована на портале № 13641

систем.

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 | Знать как выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем | Уметь выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем | Владеть способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем |
| Виды занятий | • Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа;<br>• Интерактивные практические занятия;<br>• Практические занятия;<br>• Контроль самостоятельной работы (курсовой проект / курсовая работа); | • Интерактивные лабораторные занятия;<br>• Интерактивные лекции;<br>• Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа;<br>• Интерактивные практические занятия;<br>• Практические занятия;<br>• Контроль самостоятельной работы (курсовой проект / курсовая работа); | • Интерактивные лабораторные занятия;<br>• Лабораторные работы;<br>• Самостоятельная работа;<br>• Интерактивные практические занятия;<br>• Контроль самостоятельной работы (курсовой проект / курсовая работа); |
| Используемые средства оценивания | • Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Конспект самоподготовки;<br>• Зачет;<br>• Курсовая работа (проект); | • Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Защита курсовых проектов (работ);<br>• Конспект самоподготовки;<br>• Зачет;<br>• Курсовая работа (проект); | • Отчет по лабораторной работе;<br>• Защита курсовых проектов (работ);<br>• Зачет;<br>• Курсовая работа (проект); |

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

Согласована на портале № 13641

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Отлично (высокий уровень) | • Знать в полном объеме как выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем; | • Уметь в полном объеме выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем; | • Владеть в полном объеме способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем; |
| Хорошо (базовый уровень) | • Знать на продвинутом уровне как выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем; | • Уметь на продвинутом уровне выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем; | • Владеть на продвинутом уровне способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем; |
| Удовлетворительно (пороговый уровень) | • Знать на базовом уровне как выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных | • Уметь на базовом уровне выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных | • Владеть на базовом уровне способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты |

Согласована на портале № 13641

| | | | |
|---|---|---|---|
| | сетей и систем; | сетей и систем; | телекоммуникационных сетей и систем; |

## 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

– 1. Secret Net – архитектура. 2. Secret Net - Защитные механизмы. 3. Secret Net - Программа оперативного управления. 4. Централизованная инвентаризация ресурсов локальной сети . 5. Централизованная защита от вирусов в локальной сети. 6. Централизованное управление средствами защиты от несанкционирован-ного доступа в локальной сети. 7. Централизованный учет и управление программно-аппаратными средства-ми защиты информации.

### 3.2 Зачёт

– 1. Для чего предназначен механизм контроля подключения и изменения устройств? 2. Для каких устройств реализован механизм контроля подключения и изменения? 3. Для чего предназначен механизм контроля целостности (КЦ)? 4. Для чего предназначен механизм замкнутой программной среды? 5. Перечислите методы контроля для КЦ. 6. Какие есть режимы для замкнутой программной среды? 7. Для чего нужен журнал событий? 8. Какой формат данных используется в журнале Secret Net? 9. Приведите несколько категорий регистрации событий 10. Кто может работать с журналом? 11. Для чего нужно теневое копирование? 12. Для каких устройств может осуществляться теневое копирование? Для чего предназначена программа оперативного управления Secret Net? 13. Какие режимы работы имеет программа оперативного управления Secret Net? 14. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме конфигурирования. 15. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме управления. 16. В какой последовательности применяются параметры групповых политик? 17. Для чего необходимо квитирование событий НСД? 18. Какие виды отчетов можно построить с помощью программы ОУ? 19. В каких случаях необходимо изменение сетевых настроек?

### 3.3 Темы опросов на занятиях

– 1. Основные функции системы КБИ. 2. Что такое Kaspersky Security Center? 3. Какие основные функции в Kaspersky Security Center? 4. Как получить информацию о конкретном компьютере в сети? 5. Что такое паспорт компьютера? 6. Для чего предназначен сайт SAM Self Service Center? 7. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме управления. 8. Какой формат данных используется в журнале Secret Net? 9. Для каких устройств реализован механизм контроля подключения и изменения? 10. Какие есть режимы для замкнутой программной среды? 11. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме конфигурирования. 12. Для чего предназначен сайт SAM Rescue Center? 13. Для чего нужны отчёты о результатах инспектирования? Какие группы отчётов предла-гаются системой КБИ? 14. Что такое «Сервер администрирования»? 15. Что такое «Удаленная установка» и как ей пользоваться?

### 3.4 Темы лабораторных работ

– “КБ Инвентаризация”. Проведение инспекций
– Управление серверами администрирования KSC
– Аутентификация в операционной системе. Разграничение доступа к данным
– Разграничение доступа к устройствам. Замкнутая программная среда. Контроль целостности
– Работа со сведениями в журнале регистрации событий. Теневое копирование
– Secret Net. Оперативное управление

Согласована на портале № 13641

– Управление жизненным циклом средств аутентификации

### 3.5 Темы курсовых проектов (работ)

– Рассмотрим задание, которое необходимо выполнить в рамках выполнения курсовой работы: 1. В соответствии с вариантом, определить информацию, обрабатываемую в автоматизированных системах организации. Определить угрозы, а также информацию, нуждающуюся в защите. 2. Объединить виртуальные машины, выданные преподавателем в домен. 3. Скачать демо-версию СЗИ от НСД Secret Net и требуемую документацию. 4. Произвести установку серверной и клиентских частей Secret Net на виртуальные машины. 5. Произвести настройку подсистем Secret Net в соответствии с вариантом (создать каталоги и файлы на виртуальных машинах, которые бы соответствовали данной информации). Сюда входит настройка, а также объяснение причин, в соответствии с которыми были настроены данные подсистемы: – Политик Secret Net. – Разграничение доступа к устройствам. – Задание мандатного или дискреционного метода управления доступом. – Настройка замкнутой программной среды (обязательна для нечетных вариантов). – Настройка контроля целостности данных (обязательна для четных вариантов). – Настройка затирания данных. – Настройка контроля печати. 6. Подготовить пояснительную записку, содержащую описание выполненных работ, а также выводы по всей работе.

## 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 фор-мирования компетенций, согласно п. 12 рабочей программы.

### 4.1. Основная литература

1. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 4-е изд., стер. - М. : Академия, 2009. - 336 с. : ил., табл. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. (наличие в библиотеке ТУСУР - 21 экз.)

### 4.2. Дополнительная литература

1. Компьютерные сети: Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2013. - 944 с. : ил., табл. - (Учебник для вузов. Стандарт третьего поколения). (наличие в библиотеке ТУСУР - 20 экз.)

2. Защита информации с использованием смарт-карт и электронных брелоков / Л. К. Бабенко, С. С. Ищуков, О. Б. Макаревич. - М. : "Гелиос АРВ", 2003. - 351[1] с. : ил., табл., портр. - Библиогр.: с. 348-349. (наличие в библиотеке ТУСУР - 30 экз.)

### 4.3. Обязательные учебно-методические пособия

1. Рахманенко И.А. Методические указания по выполнению практических работ по дисциплине Управление средствами защиты информации [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_pract.pdf

2. Рахманенко И.А. Лабораторный практикум по дисциплине “Управление средствами защиты информации” [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_lab.pdf

3. Рахманенко И.А. Методические указания для выполнения курсовой работы по дисциплине Управление средствами защиты информации [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_course.pdf

4. Рахманенко И.А. Методические указания для выполнения самостоятельной и индивидуальной работы по дисциплине Управление средствами защиты информации [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/gia/uszi_sam.pdf

### 4.4. Базы данных, информационно справочные и поисковые системы

1. Система подготовки документов Open Office; Система для использования виртуальных машин VMware Player; Google; Wikipedia.

Согласована на портале № 13641