МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Томский государственный университет систем управления и радиоэлектроники» (ТУСУР)

Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

И.А. Рахманенко

Управление средствами защиты информации

Методические указания к
самостоятельной и индивидуальной работе

Томск, 2021

Цели и задачи дисциплины

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

Задачи изучения дисциплины – получение студентами:

– Получение знаний и умений по методам сбора и аудита событий информационной безопасности в современных средствах защиты информации;

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

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

– Изучение методов контроля и оценки установленного программного и аппаратного обеспечения на защищаемых компьютерах в локальной сети;

– Изучение методов обеспечения и контроля антивирусной защиты рабочих станций в сети организации.

Самостоятельная работа включает следующие виды работ:

1. Проработка лекционного материала (проверка на зачете);
2. Подготовка к лабораторным работам (проверка на лабораторной работе);
3. Написание отчета по лабораторной работе (проверка на лабораторной работе);
4. Выполнение ИДЗ (проверка на практическом занятии).

1. Проработка лекционного материала

Темы лекций:

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 несанкционированного доступа в локальной сети.
7. Централизованный учет и управление программно-аппаратными средствами защиты информации.
8. Анализ нормативных требований по управлению средствами защиты информации.

Контрольные вопросы:

1. Для чего предназначен механизм контроля целостности (КЦ)?
2. Для чего предназначен механизм замкнутой программной среды?
3. Для каких устройств может осуществляться теневое копирование?
4. Для чего предназначена программа оперативного управления Secret Net?
5. Для чего предназначена программа SAM?
6. Для чего предназначен сайт SAM Management Center?
7. Из каких программных компонентов состоит система КБИ?
8. Основные функции системы КБИ.
9. В каких режимах может работать Kaspersky Security Center?

2. Подготовка к лабораторным работам

Самостоятельная работа в ходе подготовки к лабораторным работам включает в себя оформление отчета и повторение материала, изученного на практической работе. Темы практических занятий:

– Лабораторная работа 1. «Разграничение доступа к устройствам. Замкнутая программная среда. Контроль целостности»

– Лабораторная работа 2. «Работа со сведениями в журнале регистрации событий. Теневое копирование»

– Лабораторная работа 3. “Secret Net. Оперативное управление”

– Лабораторная работа 4. Safenet Authentication Manager (SAM) 8.0. Настройка и базовые возможности.

– Лабораторная работа 5. Система сбора данных о программном и аппаратном обеспечении «Код Безопасности: Инвентаризация»

– Лабораторная работа 6. “Kaspersky Security Center”

3. Написание отчета по лабораторной работе

Данный этап самостоятельной работы включает в себя подготовку студентом отчета по итогам выполнения лабораторной работы. Отчет должен быть оформлен согласно ОС ТУСУР 01-2013. Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления. В структуре отчета должны содержаться: титульный лист, цель лабораторной работы, индивидуальное задание, ход выполнения работы, итоги и анализ выполнения индивидуального задания по варианту.

После выполнения работы студенту необходимо оформить отчет, включающий в себя как описание хода работы, так и выполнение индивидуального задания по варианту. Помимо скриншотов в отчет должно быть включено описание произведенных действий с полученным результатом. Файл с отчетом должен быть прикреплен к соответствующему заданию в электронной образовательной среде MOODLE (sdo.tusur.ru) в формате Microsoft Word (doc,docX) или PDF. Оценивается как выполнение хода работы (50 % баллов), так и выполнение индивидуального задания (оставшиеся 50%).

4. Выполнение индивидуального домашнего задания

В ходе изучения дополнительных материалов к лекциям и лабораторным работам студентами может быть выполнено индивидуальное домашнее задание, являющееся необязательным. К самостоятельному изучению и проработке предлагаются следующие темы:

1. Централизованная инвентаризация ресурсов локальной сети.
2. Централизованная защита от вирусов в локальной сети.
3. Централизованное управление средствами защиты от несанкционированного доступа в локальной сети.
4. Централизованный учет и управление программно-аппаратными средствами защиты информации.
5. Аутентификация в операционной системе. Разграничение доступа к данным.
6. Разграничение доступа к устройствам.
7. Замкнутая программная среда.
8. Контроль целостности конфиденциальной информации.
9. Управление жизненным циклом средств аутентификации.
10. Управление серверами администрирования KSC.