МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 36»

РАССМОТРЕНО
научно-методическим советом
Протокол № 1
от 29 августа 2023 г.

УТВЕРЖДЕНО
директор школы Свешникова Л.И.
Приказ № 1144
от 30 августа 2023 г.

Рабочая программа курса по выбору учащегося Информационная безопасность для 11 класса

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Введение

Предмет, цели, содержание дисциплины. Важность и актуальность дисциплины. Роль дисциплины в формировании специалиста в соответствии с квалификационной характеристикой и образовательным стандартом. Ее место в общем комплексе дисциплин специальности и специализации. Ее взаимосвязь с другими дисциплинами примерного учебного плана. Содержание дисциплины. Виды контроля знаний.

Раздел 1. Уязвимости информационных технологий на примере интранета и Интернета

Тема 1. Основные понятия информационной безопасности (ИБ)

Уязвимость, угроза ИБ, источник угрозы ИБ, модель угроз ИБ, модель нарушителя ИБ, сетевая атака. Информационные ресурсы информационных систем (ИС) как объекты атак. Уровни информационной инфраструктуры. Объекты атак с точки зрения информационной инфраструктуры.

Тема 2. Модели угроз и нарушителей ИБ

Причины уязвимости ИС. Классификация уязвимостей. Уязвимости архитектуры клиент-сервер: конфигурация системы, уязвимость операционных систем, уязвимость серверов (уязвимость систем управления базами данных, уязвимость систем электронного документооборота), уязвимость рабочих станций, уязвимость каналов связи (перехват паролей, перехват незащищенного трафика, недостатки протоколов, уязвимости каналообразующего оборудования). Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов TCP/IP (Telnet, FTP, NFS, DNS, NIS, WorldWideWeb, команды удаленного выполнения, Sendmail и электронная почта, другие утилиты). Средства замены уязвимых сервисов TCP/IP. Слабости современных технологий программирования (Java, ActiveX) и ошибки в программном обеспечении. Виды угроз ресурсам интранета и Интернета. Виды источников угроз ИБ. Модель нарушителей ИБ. Инсайдеры и аутсайдеры. Виды ущерба объектам атак.

Раздел 2. Удаленные сетевые атаки на примере интранета и Интернета

Тема 3. Классификация типовых удаленных атак в информационных системах

Классификация удаленных атак. Анализ сетевого трафика. Подмена доверенного объекта или субъекта. Ложный объект. «Отказ в обслуживании». Удаленный контроль над станцией в сети. Типичные сценарии и уровни атак.

Тема 4. Методы взлома открытых информационных систем

Классические методы взлома (взлом парольной защиты). Современные методы взлома: перехват данных при их перемещении по каналам связи и перехват ввода с клавиатуры; мониторинг в графических интерфейсах; подмена системных утилит; нападения с использованием сетевых протоколов. Сетевые вирусы.

Раздел 3. Комплексное обеспечение ИБ

Тема № 5. Специфика защиты ресурсов информационных систем

Комплексный и фрагментарный подходы к защите ИС. Четырехуровневая модель ИБ. Эшелонированная защита ИС в целом и отдельных ее элементов. Руководящие документы и стандарты по защите ИС. Топология сети: физическая изоляция; изоляция протокола; выделенные каналы.

Тема № 6. Политика информационной безопасности

Разновидности политик ИБ. Модели доверия. Основные положения политики ИБ. Процесс выработки политики ИБ, ее реализация и модификация.

Раздел 4. Средства обеспечение информационной безопасности информационных систем

Тема № 7. Сервисы безопасности в информационных системах

Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры. Подсистемы ИБ.

Тема № 8. Примеры средств обеспечения информационной безопасности для информационных систем

Аутентификация в сетях: обычные и одноразовые пароли; серверы аутентификации. Защита Web-технологии. Защита электронной почты.

Тема № 9. Навыки безопасной работы в Интернете

Дополнительная информация и итоговые рекомендации по защите ОИС.

Заключение

История и перспективы информационных систем в мире. Современное состояние открытых информационных систем в России. Перспективы открытых информационных систем в России.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

Номер раздела / темы	Часы (академические), отведенные на изучение раздела (темы)	
	занятия лекционного типа	лабораторные работы
1	2	3
Введение	1	-
Раздел 1 / Тема 1	2	-
Раздел 1 / Тема 2	6	4
Раздел 2 / Тема 3	4	-
Раздел 2 / Тема 4	4	4
Раздел 3 / Тема 5	4	-
Раздел 3 / Тема 6	6	8
Раздел 4 / Тема 7	4	4
Раздел 4 / Тема 8	4	6
Раздел 4 / Тема 9	4	6
Заключение	1	-

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Общие рекомендации при изучении материала

При повторении материала целесообразно придерживаться следующей последовательности:

Ориентировка. Прочитать текст с целью понять его главные положения. Если требуется, подчеркнуть их, выписать, повторить в памяти.

Чтение. Прочитать текст еще раз очень внимательно и постараться выделить второстепенные детали. Установить связь между ними и главными положениями. Несколько раз повторить в памяти главные положения в их связи с второстепенными деталями.

Обзор. Быстро просмотреть текст. Проверить, правильно ли сделаны выводы о связи главных положений с соответствующими второстепенными деталями. Для более глубокого понимания текста поставить вопросы к его основным научным положениям.

Главное. Мысленно пересказать текст или пересказать его кому-нибудь вслух, вспоминая при этом главные положения. Дать ответы на поставленные вопросы.

При необходимости сделать короткий перерыв в работе над текстом, при этом следует соблюдать следующее правило. Он должен совпадать с окончанием предложения, а еще лучше – абзаца. Более длительные перерывы целесообразно устраивать после прочтения целиком параграфа или главы книги.

Рекомендации по осмыслению изучаемого материала

1. Постановка вопросов к самому себе и поиск ответов на них либо в тексте, либо путем вспоминания и рассуждения.

2. Предвосхищение плана изложения текста. Этот прием позволяет читающему как бы войти в творческую лабораторию автора, выдвигать гипотезы, предвидеть логический план содержания книги.

3. Предугадывание содержания, то есть определение того, что именно будет сказано дальше. Использование этого приема предполагает наличие у читателя определенной суммы знаний в данной области. Одновременно происходит формирование умений доказывать, обосновывать свою мысль, строить цепь рассуждений и фактов, то есть развиваются способности к научной работе.

4. Мысленное возвращение к ранее прочитанному под влиянием новой мысли для более углубленного осмысливания отдельных положений.

5. Критический анализ текста и оценка его. Тут предполагается целая система приемов, которая вызывает появление дополнений к изучаемому тексту, формирование своего мнения, отстаивание своей точки зрения.

Для понимания текста может оказаться успешным метод, связанный с образным представлением читаемого текста. В ходе чтения важное значение имеет умение определять роль отдельных частей текста, устанавливать их соподчиненность (глав, параграфов, рубрик), находить взаимосвязь текста с рисунками, таблицами, графиками, сносками, примечаниями и приложениями.

Введение

Предмет, цели, содержание дисциплины. Важность и актуальность дисциплины. Роль дисциплины в формировании специалиста в соответствии с квалификационной характеристикой и образовательным стандартом. Ее место в общем комплексе дисциплин специальности и специализации. Ее взаимосвязь с другими дисциплинами примерного учебного плана. Содержание дисциплины. Виды контроля знаний.

Задание:

1. По рекомендованной литературе изучить Л.1, гл.1.
2. Повторить лекцию № 1.

Раздел 1. Уязвимость ОИС на примере интранета и Интернета

Тема 1. Основные понятия информационной безопасности открытых систем

Уязвимость, угроза ИБ, источник угрозы ИБ, модель угроз ИБ, модель нарушителя ИБ, сетевая атака. Информационные ресурсы открытых ИС как объекты атак. Уровни информационной инфраструктуры. Объекты атак с точки зрения информационной инфраструктуры.

Задание

1. По рекомендованной литературе изучить Л.1, разд.2.1 – 2.3.

2. Повторить лекции № 1, 2.
3. Подготовить отчёт по лабораторной работе №1

Тема 2. Модели угроз и нарушителей ИБоткрытых информационных систем

Причины уязвимости ИС. Классификация уязвимостей. Уязвимости архитектуры клиент-сервер: конфигурация системы, уязвимость операционных систем, уязвимость серверов (уязвимость систем управления базами данных, уязвимость систем электронного документооборота), уязвимость рабочих станций, уязвимость каналов связи (перехват паролей, перехват незащищенного трафика, недостатки протоколов, уязвимости каналообразующего оборудования). Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, WorldWideWeb, команды удаленного выполнения, Sendmail и электронная почта, другие утилиты). Средства замены уязвимых сервисов TCP/IP. Слабости современных технологий программирования (Java, ActiveX…) и ошибки в программном обеспечении. Виды угроз ресурсам интранета и Интернета. Виды источников угроз ИБ. Модель нарушителей ИБ. Инсайдеры и аутсайдеры. Виды ущерба объектам атак.

Задание

1. По рекомендованной литературе изучить Л.1, разд.3.1 – 3.3
2. Повторить лекции № 3, 4.
3. Подготовить отчёт по лабораторной работе №2

Раздел 2. Удаленные сетевые атаки на ОИС на примере интранета и Интернета

Тема 3. Классификация типовых удаленных атакв открытых информационных системах

Классификация удаленных атак. Анализ сетевого трафика. Подмена доверенного объекта или субъекта. Ложный объект. "Отказ в обслуживании". Удаленный контроль над станцией в сети. Типичные сценарии и уровни атак.

Задание

1. По рекомендованной литературе изучить Л.1, разд.3.4 – 3.5.
2. Повторить лекции № 5,6.

Тема 4. Методы взлома открытых информационных систем

Классические методы взлома (взлом парольной защиты). Современные методы взлома: перехват данных при их перемещении по каналам связи и перехват ввода с клавиатуры; мониторинг в графических интерфейсах; подмена системных утилит; нападения с использованием сетевых протоколов. Сетевые вирусы.

Задание

1. По рекомендованной литературе изучить Л.1, разд.3.4 – 3.5.
2. Повторить лекции № 7
3. Подготовить отчёты по лабораторным работам №3

Раздел 3. Комплексное обеспечение ИБ ОИС

Тема № 5. Специфика защиты ресурсов открытых информационных систем

Комплексный и фрагментарный подходы к защите ИС. Четырехуровневая модель ОИС. Эшелонированная защита ОИС в целом и отдельных ее элементов. Руководящие документы и стандарты по защите ОИС. Топология сети: физическая изоляция; изоляция протокола; выделенные каналы.

Задание

1. По рекомендованной литературе изучить Л.1, разд.4.1 – 4.5.
2. Повторить лекции № 8, 9.
3. Подготовить отчёт по лабораторной работе №4

Тема № 6. Политика информационной безопасности для открытых информационных систем

Разновидности политик ИБ. Модели доверия. Основные положения политики ИБ. Процесс выработки политики ИБ, ее реализация и модификация.

Задание

1. По рекомендованной литературе изучить Л.1, разд.4.1 – 4.5.
2. Повторить лекции № 10.
3. Подготовить отчёт по лабораторной работе №4

Раздел 4. Средства обеспечение информационной безопасностиоткрытых информационных систем

Тема № 7. Сервисы безопасности воткрытых информационных системах

Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры. Подсистемы ИБ.

Задание

1. По рекомендованной литературе изучить Л.1, разд.5.1 – 5.3.
2. Повторить лекции № 11, 12.
3. Подготовить отчёт по лабораторной работе №5

Тема № 8. Примеры средств обеспечения информационной безопасности для открытых информационных систем

Аутентификация в сетях: обычные и одноразовые пароли; серверы аутентификации. Защита Web-технологии. Защита электронной почты.

Задание

1. По рекомендованной литературе изучить Л.1, разд.5.2 – 5.5.
2. Повторить лекции № 13- 15.
3. Подготовить отчёт по лабораторной работе №6

Тема № 9. Навыки безопасной работы в Интернете

Дополнительная информация и итоговые рекомендации по защите ОИС.

Задание

1. По рекомендованной литературе изучить Л.1, разд.6.1 – 6.3.
2. Повторить лекции № 16, 17.
3. Подготовить отчёт по лабораторной работе №7

Заключение

История и перспективы открытых информационных систем в мире. Современное состояние открытых информационных систем в России. Перспективы открытых информационных систем в России.

ОРГАНИЗАЦИЯ ТЕКУЩЕГО КОНТРОЛЯ

По дисциплине предусмотрены лабораторные работы, в ходе проведения которых осуществляется текущий контроль.

Перечень лабораторных работ:

Номер раздела / темы	Тема лабораторной работы
2	**3**
Раздел 1/Тема 2	Лабораторная работа 1 (ЛР1) Определение показателей защищенности при НСД к информации
Раздел 2/Тема 4	Лабораторная работа 2 (ЛР2). Оценка эффективности систем защиты

	программного обеспечения.
Раздел 3/Тема 6	Лабораторная работа 3 (ЛР3). Доказательство алгоритмической неразрешимости проблемы безопасности с использованием модели HRU. Правила передачи прав доступа в модели Take-Grant.
Раздел 3/Тема 6	Лабораторная работа 4 (ЛР4). Расширенная модель Белла–Лападула и анализ путей возникновения информационных каналов
Раздел 4/Тема 7-9	Лабораторная работа 5 (ЛР5). Парольные системы защиты автоматизированных систем
Раздел 4/Тема 7-9	Лабораторная работа 6 (ЛР6). Система защиты информации от несанкционированного доступа DallasLock 7.7.
Раздел 4/Тема 7-9	Лабораторная работа 7 (ЛР7). Межсетевые экраны автоматизированных систем.

Лабораторная работа №1. (ЛР1)
Тема: Определение показателей защищенности при НСД к информации
*Цель работы:*выработка практических умений и приобретение навыков в определении показателей защищенности при НСД к информации.
Исполнение.

1. Методика определения показателей защищенности при НСД к информации.
2. Решение задач по определения показателей защищенности при НСД.
3. Выполнение индивидуального задания

Оценка. Формирование навыков и опыта практической работы поопределение показателей защищенности при НСД к информации. Оцениваниепо результатам выполнения заданий лабораторной работы.
Время выполнения работы: 4 часа

Лабораторное занятие №2 (ЛР2)
*Тема:*Оценка эффективности систем защиты программного обеспечения
Цель работы: выработка практических умений и приобретение навыков в оценке эффективности систем защиты программного обеспечения.

1. Системы защиты программного обеспечения. Достоинства и недостатки основных СЗИ
2. Показатели эффективности систем защиты
3. Выполнение индивидуального задания

Оценка. Формирование навыков и опыта практической работы пооценке эффективности систем защиты программного обеспечения. Оцениваниепо результатам выполнения заданий лабораторной работы.
Время выполнения работы: 4 часа

Лабораторная работа №3. (ЛР3)
Тема: Доказательство алгоритмической неразрешимости проблемы безопасности с использованием модели HRU. Правила передачи прав доступа в модели Take-Grant.
Цель работы: изучение особенностей моделей дискреционной политики безопасности HRU и Take-Grant.
Исполнение.

1. Принцип модификации матрицы доступа в модели HRU.
2. Доказательство алгоритмической неразрешимости проблемы безопасности с использованием модели HRU
3. Правила передачи прав доступа в модели Take-Grant.
4. Выполнение индивидуального задания.

Оценка. Формирование навыков и опыта практической работы пореализации дискреционной политики безопасности. Оцениваниепо результатам выполнения заданий лабораторной работы.

Время выполнения работы: 6 часа

Лабораторная работа №4. (ЛР4)
*Тема:*Расширенная модель Белла–Лападула и анализ путей возникновения информационных каналов
Цель работы: изучение особенностей реализации расширенной модели Белла–Лападула и анализ путей возникновения информационных каналов
Исполнение.

1. Разграничение доступа в модели Белла–Лападула.
2. Работа с программным обеспечением «Ревизор-1XP».
3. Работа с программным обеспечением «Ревизор-2XP».
4. Выполнение индивидуального задания.

*Оценка.*Формирование навыков и опыта практической работы пореализации мандатной политики безопасности. Оцениваниепо результатам выполнения заданий лабораторной работы.
Время выполнения работы: 6 часа

Лабораторная работа №5. (ЛР5)
Тема: Парольные системы защиты автоматизированных систем
*Цель работы:*привитие практических умений и приобретение навыков в использовании парольных систем защиты в автоматизированных системах.
Исполнение.

1. Назначение и характеристики систем парольной защиты
2. Изучение принципов функционирования систем парольной защиты*Scarabay 2.8* и*VipNet.*
3. Инсталляция, настройка и сравнение характеристик парольных систем
4. Выполнение индивидуального задания.

Оценка. Формирование навыков и опыта практической работы в использовании парольных систем защиты в автоматизированных системах. Оцениваниепо результатам выполнения заданий лабораторной работы.
Время выполнения работы: 4 часа

Лабораторное занятие №6. (ЛР6)
Тема:«Система защиты информации от несанкционированного доступа DallasLock 7.7»
Цель работы: Рассмотреть механизм автоматизированной проверки соответствия прав пользователей по доступу к защищаемым информационным ресурсам АРМ.
Исполнение.

1. Назначение и условия применения программы
2. Входные и выходные данные. Состав и функции программного средства DallasLock 7.7
3. Выполнение индивидуального задания.

*Оценка.*Формирование навыков и опыта практической работы в проверке соответствия прав пользователей по доступу к защищаемым информационным ресурсам АРМ. Оцениваниепо результатам выполнения заданий лабораторной работы.
Время выполнения работы: 6 часа

Лабораторное занятие №7.(ЛР7)
Тема: Межсетевые экраны автоматизированных систем
Цель работы: изучение особенностей загрузки, конфигурирования и функционирования межсетевых экранов автоматизированных систем.
Исполнение.

1. Назначение и характеристики межсетевых экранов
2. Инсталляция, настройка и сравнение характеристик межсетевых экранов

3. Выполнение индивидуального задания.

Оценка. Формирование навыков и опыта практической работы в проверке соответствия прав пользователей по доступу к защищаемым информационным ресурсам АРМ. Оцениваниепо результатам выполнения заданий лабораторной работы.

Время выполнения работы: 6 часа

ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

Основная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — М. : Издательство Юрайт, 2018. — 309 с. — (Серия : Бакалавр и магистр.академический курс). — ISBN 978-5-534-04732-5. — Режим доступа :www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E.

2. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб.пособие — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана. (http://www.iprbookshop.ru/63594.html)

3. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем Учебник для вузов в 2-х томах (с грифом Минобразования и науки РФ). Том 1 – Угрозы, уязвимости, атаки и подходы к защите.). Том 2 – Средства защиты в сетях.- М.: Горячая линия-Телеком, 2013, 538 с. Режим доступа: http://www.iprbookshop.ru/63594.html

Дополнительная литература

1. Мельников, Д.А. Информационная безопасность открытых систем [Электронный ресурс] : учеб. — Электрон.дан. — Москва : ФЛИНТА, 2014. — 448 с. — Режим доступа: https://e.lanbook.com/book/48368. — Загл. с экрана.

2. Галатенко, В.А. Стандарты информационной безопасности [Электронный ресурс] : учеб.пособие — Электрон. дан. — Москва : Национальный Открытый Университет "ИНТУИТ", 2016. — 307 с. — Режим доступа: https://e.lanbook.com/book/100511. — Загл. с экрана.

Периодическая литература

1. Журнал "Информационная безопасность" (www.securitylab.ru);
2. Журнал "Системы безопасности" (www.securitylab.ru);
3. Журнал "Защита информации. Инсайд"(www.securitylab.ru);
4. Журнал "БДИ"(Безопасность. Достоверность. Информация)(www.securitylab.ru)

Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru

Справочно-правовая система «Консультант+» http://www.consultant-urist.ru

Справочно-правовая система «Гарант» http://www.garant.ru

База данных Web of Science https://apps.webofknowledge.com/

База данных Scopus https://www.scopus.com

Портал открытых данных Российской Федерации https://data.gov.ru

База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata

База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/

База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/

Базы данных Министерства экономического развития РФ http://www.economy.gov.ru
База открытых данных Росфинмониторинга http://www.fedsfm.ru/opendata
Электронная база данных «Издательство Лань» https://e.lanbook.com
Электронная библиотечная система «IPRbooks» http://www.iprbookshop.ru
База данных «Электронно-библиотечная система «ЭБС ЮРАЙТ» https://www.biblio-online.ru
База данных электронно-библиотечной системы ТГТУ http://elib.tstu.ru
Федеральная государственная информационная система «Национальная электронная библиотека» https://нэб.рф
Национальный портал онлайн обучения «Открытое образование» https://openedu.ru
Электронная база данных "Polpred.com Обзор СМИ" https://www.polpred.com
Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Наряду с представлением основного содержания и особенностей изучаемого курса в процессе подготовки специалистов в области информационной безопасности автоматизированных систем, ознакомить студентов с историей развития информационных технологий, базовыми информационными технологиями и их местом в системах автоматизированного управления.

Курс состоит из лекций, на которых раскрывают основные проблемные вопросы по каждой теме, лабораторных работ, на которых проводится практическое изучение и исследование отдельных вопросов, рассмотренных в ходе предыдущих лекций и самостоятельной работы.

В процессе преподавания дисциплины возможно использование следующих технологий образовательного процесса:

1. Технология презентации знаний (основана на поведении преподавателя, в которой преобладает приоритет и опора на методические приёмы преподнесения знаний).
2. Технократическая технология (приоритет отдается использованию технических средств, особенно персонального компьютера). Система формализации знаний, запрограммированных форм и методов проведения занятий, жесткого регламента.
3. Технология адаптивного типа (предполагает регулярную корректировку форм занятий и стилей обучения).
4. Технология социально-психологического типа (использование социально-психологических характеристик восприятия личностью и группой определенного объема знаний и методов обучения, восприятия преподавателя студентами и т.д.).
5. Технология креативного обучения (используется творческий потенциал личности, способность к творчеству, к неординарному восприятию материала и т.д.). Основное– постановка проблем, обсуждение их содержания.
6. Технология самообразования (самостоятельное освоение отдельных разделов предмета, роль преподавателя – консультационная).

Наряду с традиционными и дидактическими методами также рекомендуется широко использовать следующие методы обучения студентов:

1. Проблемно-развивающие;
2. Исследование и анализ накопленной информации.

Это позволит улучшить уровень профессиональных знаний, их структуру, даст студентам навыки интегрированного использования знаний при решении определенных проблем в сфере информационного систем и технологий, обеспечит устойчивость знаний.

Исходя из вышесказанного, преподаватели, проводящие лекционные занятия должны раскрыть в процессе чтения лекций основные проблемные вопросы по каждому

разделу лекционного материала. Текст курса лекций имеется на кафедре в материалах УМКД.

Преподаватель может по своему усмотрению изменять конкретное содержание читаемого курса в пределах, определенных рабочей программой курса с учетом реального уровня знаний студентов и новых информационных материалов, представляющих ценность при раскрытии содержания отдельных его разделов и тем.

Для более эффективного проведения лекций рекомендуется предоставлять студентам раздаточный материал со всеми, необходимыми для эффективного прослушивания лекций графическими материалами. При возможности в процессе чтения лекций могут быть использованы мультимедийные приложения (презентации, фильмы и др.), специально подготовленные для этих целей.

С целью расширения лекционного материала, преподаватель может передавать студентам дополнительный раздаточный материал (в форме текстовой информации) для самостоятельного ознакомления с ним студентов по отдельным разделам курса. Это даст возможность студентам глубже ознакомиться с отдельными важными вопросами курса, не охватываемыми во время аудиторных занятий.

Лабораторные работы по курсу ««Информационная безопасность открытых систем»» включают занятия в компьютерной аудитории по закреплению знаний по выделенным темам в соответствии с программой курса. Занятия проводятся в форме выполнения практических заданий с элементами исследования и ответов на контрольные вопросы.

Самостоятельная работа студентов направлена на более глубокое изучение студентами отдельных вопросов курса с использованием рекомендуемой основной и дополнительной литературы и других информационных источников и включает:

- дополнительное углубленное изучение лекционных материалов по записям прочитанных лекций и представленного раздаточного материала по тематике курса;
- самостоятельное изучение студентами отдельных вопросов, связанных с отдельными частями курса. Перечень вопросов по каждой теме приведен в методических рекомендациях для выполнения самостоятельной работы студентами. Необходимые для самостоятельной работы информационные материалы предоставляются студентам в электронном виде;
- подготовка к лабораторным работам по предусмотренным программой темам. Перечень тем лабораторных работ и требования к их содержанию и оформлению приведен в методических рекомендациях по выполнению лабораторных работ;
- формирование неясных вопросов для их рассмотрения во время лекционных и практических занятий с помощью преподавателя.

Для более глубокого изучения курса преподаватель может предлагать студентам в рамках СРС подготовку устных сообщений и подготовку презентаций. Примеры некоторых тем сообщений и презентаций по рассматриваемой дисциплине приведены в методических рекомендациях по выполнению самостоятельной работы студентов.

Форму оценки и контроля СРС преподаватель выбирает самостоятельно в зависимости от индивидуальных качеств обучаемого и выбранной формы организации самостоятельной работы.