Направление подготовки 10.04.01 «Информационная безопасность»
Магистерская программа «Безопасность автоматизированных систем»
Методическое обеспечение для РПД Б1.О.07
«Защищенные информационные системы»

Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 10.04.01. «Информационная безопасность»

Профиль: «Безопасность автоматизированных систем»

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2023

Смоленск

Методические материалы составил:

_____ к.т.н., доцент А.В. Полячков
подпись ФИО

«20» января 2023 г.

Заведующий кафедрой «Вычислительной техники»:

_____ д.т.н., профессор А.С. Федулов
подпись ФИО

«26» января 2023 г.

Направление подготовки 10.04.01 «Информационная безопасность»
Магистерская программа «Безопасность автоматизированных систем»
Методическое обеспечение для РПД Б1.О.07
«Защищенные информационные системы»

СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 1											Семестр 2											Итого за курс											Каф.	Семестр
			Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель		
				Всего	Контакт.	Лек	Лаб	Пр	КРП	СР	Контроль				Всего	Контакт.	Лек	Лаб	Пр	КРП	СР	Контроль				Всего	Контакт.	Лек	Лаб	Пр	КРП	СР	Контроль	Всего			
7	Б1.О.07	Защищенные информационные системы												Эк РГР	**144**	52	18	34			56	36	4		Эк РГР	**144**	52	18	34			56	36	4		15	2

ОБОЗНАЧЕНИЯ:

Виды промежуточной аттестации (виды контроля):

Экз - экзамен;
ЗаО - зачет с оценкой;
За – зачет.

Виды работ:

Контакт. – контактная работа обучающихся с преподавателем;
Лек. – лекционные занятия;
Лаб.– лабораторные работы;
Пр. – практические занятия;
КРП – курсовая работа (курсовой проект);
РГР – расчетно-графическая работа (реферат);
СР – самостоятельная работа студентов;
з.е.– объем дисциплины в зачетных единицах.

Содержание дисциплины:

№	Наименование видов занятий и тематик, содержание
1	**Лекционные занятия** – 9 шт. по 2 часа. Тема 1. Анализ угроз информационной безопасности 1.1. Проблемы безопасности информационных систем (2 часа). Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Проблемы безопасности IP-сетей. Способы обеспечения информационной безопасности. Пути решения проблемы защиты информации. Тема 2. Политика безопасности. 1.2. Основные понятия политики безопасности. (2 часа). Описание проблемы. Область применения. Позиция организации. Распределение ролей и обязанностей. Управленческие меры обеспечения информационной безопасностью. 1.3. Структура политики безопасности организации (2 часа). Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Тема 3. Архитектура защищенной информационной системы 1.4. Концепция глобального управления безопасностью (2 часа). Концепция GSM (Global Security Management). Основные свойства GSM. Глобальная и локальная политика безопасности. 1.5. Функционирование системы управления средствами безопасности. (2 часа). Назначение основных средств безопасности. Защита ресурсов. Управление средствами защиты. Управление пользователями и правами доступа. Аудит и мониторинг безопасности информационных систем. 1.6. Обеспечение безопасности облачных систем (2 часа). Общие требования к безопасности облачных технологий. Безопасность сетевой части облака. Безопасность серверной части облака. Безопасность хранения данных и приложений. 1.7. Средства защиты информационных систем (2 часа). Организация защиты от вирусов. Межсетевые экраны. Средства обнаружения и предотвращения вторжений. Средства предотвращения утечек. Средства шифрования. Средства двухфакторной аутентификации. Однократная аутентификация. Ложные информационные системы. Тема 4. Тестирование защиты 1.8. Модель опасностей (2 часа). Декомпозиция приложения. Ранжирование интерфейсов по степени уязвимости. Атаки по классификации STRIDE. Создание инструментов для поиска дефектов. 1.9. Создание тест-планов на основании модели опасностей (2 часа). Создание тест-плана. Определение «поверхности поражения». Определение основных векторов атаки. Тестирование с шаблонами безопасности. Сквозное тестирование.
2	**Лабораторные работы** – 4 шт. по 8 часов и 1 – 2 часа. 2.1. Установка защищенной информационной системы. Цель лабораторной работы: Провести установку программного обеспечения криптошлюза и настройку сетевого взаимодействия между ним и центром управления сетью. 2.2. Настройка правил фильтрации, разрешающих прохождение трафика между компьютерами из защищаемой сети и сети общего доступа. Цель лабораторной работы: Демонстрация настроек межсетевого экрана 2.3 Настройка правила фильтрации, разрешающего прохождение трафика между компьютерами из внутренних сетей, защищаемых разными криптошлюзами. 2.4 Мониторинг состояния компонентов системы и передаваемого трафика, настройка реакции на события. 2.5. Средства обнаружения и предотвращения вторжений.

№	Наименование видов занятий и тематик, содержание
3	**Расчетно-графическая работа** «Разработка модели защищенной информационные системы». Выполнение индивидуального задания, предполагающего разработку модели защищенной информационной системы, реализацию и проверку ее работы.
4	**Самостоятельная работа** студентов: 4.1. Подготовка к защите лабораторных работ. 4.2. Самостоятельное изучение теоретических материалов по следующим вопросам. Методы оценки рисков информационной безопасности (ИБ). Процесс оценки рисков ИБ: идентификация рисков, анализ рисков, оценивание рисков, обработка рисков. Процесс управления риском ИБ. Программный инструментарий для управления рисками. Методика CRAMM. Методика ГРИФ. Методика RiskWatch. Методика CORAS. Методика MSAT. 4.3. Выполнение расчетно-графической работы.

Текущий контроль:
- проверка конспектов лекций;
- проверка отчетов по лабораторным работам; защита лабораторных работ;
- консультации и контроль выполнения расчетно-графической работы

Результаты текущего контроля фиксируются с использованием трехбалльной системы (0, 1, 2) при проведении контрольных недель по графику филиала в течение семестра, а также учитываются преподавателем при осуществлении промежуточной аттестации по настоящей дисциплине.

К промежуточной аттестации студентов по дисциплине могут привлекаться представители работодателей, преподаватели последующих дисциплин, заведующие кафедрами.

Оценка качества освоения дисциплины включает как текущий контроль успеваемости, так и промежуточную аттестацию.

Оценочные средства текущего контроля успеваемости:

Вопросы для защиты лабораторных работ

***Лабораторная работа* «Установка защищенной информационной системы».**

1. Для чего предназначен аппаратно-программный комплекс криптошифрования?
2. Что такое криптографический шлюз?
3. Какие действия может выполнять криптошлюз при обработке IP-пакетов?
4. Что такое идентификатор криптошлюза?
5. Какие криптошлюзы могут иметь одинаковый идентификатор?

***Лабораторная работа* «Настройка правил фильтрации, разрешающих прохождение трафика между компьютерами из защищаемой сети и сети общего доступа».**

1. Какие функции выполняет межсетевой экран?
2. Для чего предназначена технология "Контроль состояния соединений" в пакетном фильтре, применяемом в АПКШ ?

***Лабораторная работа* «Настройка правила фильтрации, разрешающего прохождение трафика между компьютерами из внутренних сетей, защищаемых разными крипто-шлюзами».**

1. Благодаря какой технологии межсетевой экран предотвращает атаки, блокирующие доступ пользователей к ресурсам VPN?
2. Что происходит с IP-пакетами, если по правилам фильтрации их прохождение запрещено, а межсетевой экран установлен в мягком режиме?

***Лабораторная работа* «Мониторинг состояния компонентов системы и передаваемого трафика, настройка реакции на события».**

1. С помощью какой программы осуществляется загрузка записей журналов комплекса из БД ЦУС для просмотра администратором?
2. Данные с каких устройств АПКШ отражает ППЖ?
3. Какие регистрационные журналы содержит ППЖ?
4. Можно ли из ПУ ЦУС проверить соединение с каким-либо узлом сети?
5. Можно ли из ПУ ЦУС определить маршрут к определенному узлу сети?

Оценочные средства для расчетно-графической работы

Когда расчетно-графическая работа полностью выполнена и оформлена, то она сдается в печатном и электронном виде на проверку. Также для проверки представляется сама разработанная модель защищенной информационной системы Требования к содержанию и оформлению расчетно-графической работы приведены в методических указаниях по РГР.

По итогам проверки преподавателем расчетно-графической работы и разработанной практической модели студенту могут быть заданы вопросы, на которые необходимо получить ответы.

Оценочные средства для промежуточной аттестации:

Примеры вопросов к экзамену по дисциплине:

1. Угрозы и уязвимости проводных корпоративных сетей.
2. Угрозы и уязвимости беспроводных сетей.
3. Проблемы безопасности IP-сетей.
4. Способы обеспечения информационной безопасности.
5. Пути решения проблемы защиты информации
6. Основные понятия политики безопасности.
7. Распределение ролей и обязанностей.
8. Управленческие меры обеспечения информационной безопасностью.
9. Проблемы реализации политики безопасности. Политика безопасного администрирования
10. Концепция GSM (Global Security Management). Основные свойства GSM.
11. Глобальная и локальная политика безопасности. Назначение основных средств безопасности.
12. Защита ресурсов.
13. Управление средствами защиты.
14. Управление пользователями и правами доступа.
15. Аудит и мониторинг безопасности информационных систем.
16. Общие требования к безопасности облачных технологий.

17. Безопасность сетевой части облака.
18. Безопасность серверной части облака. Безопасность хранения данных и приложений.
19. Организация защиты от вирусов.
20. Межсетевые экраны.
21. Средства обнаружения и предотвращения вторжений.
22. Средства предотвращения утечек.
23. Средства шифрования.
24. Средства двухфакторной аутентификации.
25. Однократная аутентификация.
26. Ложные информационные системы.
27. Процесс оценки рисков ИБ: идентификация рисков, анализ рисков, оценивание рисков, обработка рисков.
28. Процесс управления риском ИБ
29. Методика оценки рисков ИБ CRAMM.
30. Методика оценки рисков ИБ ГРИФ.
31. Методика оценки рисков ИБ RiskWatch.
32. Методика оценки рисков ИБ CORAS.
33. Методика оценки рисков ИБ MSAT
34. Тестирование безопасности. Создание тест-плана.
35. Тестирование безопасности. Определение «поверхности поражения».
36. Тестирование безопасности. Определение основных векторов атаки.
37. Тестирование с шаблонами безопасности. Сквозное тестирование.

Пример практических заданий, выносимых на экзамен, для проверки практических умений и навыков студентов по дисциплине

Задача № 1

Имеется информационная система, состоящая из двух групп пользователей и администратора. У каждой группы пользователей свой каталог и пользователи должны иметь доступ к сетевому принтеру и модему. Администратор имеет полный доступ ко всем сетевым ресурсам (каталогам групп, системному каталогу, сканеру, принтеру, модему). В системе предусмотрены следующие права доступа – чтение, запись, выполнение. Определите список объектов и субъектов данной вычислительной системы. Составьте матрицу доступа.

Задача № 2

Имеется некоторая информационная система, построенная в соответствии с мандатной моделью безопасности Бела –Лападулла. Пользователь, работающий в данной системе и имеющий уровень доступа «С» (СЕКРЕТНО), пытается прочитать файл, имеющий уровень секретности «К» (КОНФИДЕНЦИАЛЬНО). Возможна ли данная операция? И если не возможна, то какое правило модели Бела-ЛаППадулла она нарушает. Если возможно, то, в соответствии с каким правилом.

Задача № 3

Имеется некоторая информационная система, построенная в соответствии с мандатной моделью безопасности Бела –Лападулла. Пользователь, работающий в данной системе, пытается удалить в корзину какой-либо файл, имеющий уровень секретности «СС». Возможна ли данная операция? И если не возможна, то, какое правило модели Бела-Лападулла она нарушает. Если возможно, то, в соответствии с каким правилом.

Формы промежуточной аттестации по настоящей дисциплине – **экзамен**.

Основная литература

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учебное пособие. — Москва : Горячая линия-Телеком, 2017. — 338 с. — Режим доступа: https://e.lanbook.com/book/111049.

2. Новиков В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс] : учебное пособие / В.К. Новиков. —Москва : Горячая линия-Телеком, 2017. — 176 с. — Режим доступа: https://e.lanbook.com/book/111084.

3. Щеглов А.Ю. Математические модели и методы формального проектирования систем защиты информационных систем [Электронный ресурс] : учебное пособие / А.Ю. Щеглов, К.А. Щеглов. Санкт-Петербург : НИУ ИТМО, 2015. — 93 с. — Режим доступа: https://e.lanbook.com/book/70897.

4. Ачилов Р.Н. Построение защищенных корпоративных сетей. – М.: ДМК Пресс, 2013. 250 с. – Режим доступа: https://e.lanbook.com/book/66472?category=1547

Дополнительная литература

1 . Ковалев Д.В. Информационная безопасность [Электронный ресурс] : учебное пособие / Д.В. Ковалев, Е.А. Богданова. — Ростов-на-Дону : Издательство Южного федерального университета, 2016. — 74 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=493175.

2 . Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс] : учебное пособие. — Москва : Издательский дом Высшей школы экономики, 2015. — 574 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=440285.

3 . Панкратова Е.А. Методическое обеспечение по дисциплине «Защищенные информационные системы» [Электронный ресурс]: электронные методическое обеспечение для студентов, обучающихся по направлению 10.04.01 «Информационная безопасность»/ Панкратова Е.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины

1 Справочная правовая система Консультант плюс [электронный ресурс] — Режим доступа : http://www.consultant.ru/online/.

2 Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [электронный ресурс] — Режим доступа : http://government.ru/department/387/events/.

3 Официальный сайт Росстата [электронный ресурс] — Режим доступа : www.gks.ru/.

4 20 интернет-ресурсов для специалистов по информационной безопасности // официальный сайт компании «ГЕОЛАЙН Технологии» [электронный ресурс] — Режим доступа : http://geoline-tech.com/top-20-sites-about-information-security/.

5 Полезные сайты и инструменты// Информационная безопасность. Практика информационной безопасности [электронный ресурс] — Режим доступа : http://dorlov.blogspot.com/p/blog-page_3151.html.

6 Информационная безопасность [электронный ресурс] — Режим доступа : http://www.securrity.ru/.

7 30 ресурсов по безопасности, которые точно пригодятся [электронный ресурс] — Режим доступа : https://proglib.io/p/information-security-guide/

8 Информационная безопасность. Защита данных // habr - веб-сайт в формате коллективного блога с элементами новостного сайта [электронный ресурс] — Режим доступа : https://habr.com/ru/hub/infosecurity/.

9 База Знаний Клуба Информационной безопасности [электронный ресурс] — Режим доступа : http://wiki.informationsecurity.club/doku.php/main.

10 Информационная безопасность. Защита данных [электронный ресурс] — Режим доступа : http://all-ib.ru/

Список авторских методических разработок

Методическое обеспечение по дисциплине «Защищенные информационные системы» включает также следующие авторские разработки преподавателей кафедры:

1. Панкратова Е.А. Методическое обеспечение по дисциплине «Защищенные информационные системы» [Электронный ресурс]: электронные методическое обеспечение для студентов, обучающихся по направлению 10.04.01 «Информационная безопасность»/ Панкратова Е.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019.

- комплект лекций в формате мультимедийных презентаций;
- учебно-методические материалы размещены на ресурсах кафедры.