МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ

Декан факультета
информационных технологий
/Д. Г. Демидов/

"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защищенные информационные системы

Направление подготовки
10.04.01 Информационная безопасность

Профиль
Системы управления информационной безопасностью

Квалификация
Магистр

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Доцент кафедры «Информационная безопасность» /И.В. Калуцкий/
к.т.н., доцент

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,
/А.Ю. Гневшев

Руководитель образовательной программы
Доцент. к.т.н. /С.А. Кесель/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

Цель дисциплины:

Изучение технологий, методов и средств создания защищенных информационных систем для успешной профессиональной деятельности.

Задачи дисциплины:

1. Формирование профессиональной культуры обеспечения информационной безопасности (ИБ) в ИС.
2. Изучение принципов построения защищенных ИС.
3. Ознакомление с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС.
4. Изучение подходов и методов обеспечения ИБ ИС.

Планируемые результаты обучения

Обучение по дисциплине «Защищенные информационные системы» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.1. Умеет: разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.
ПК-2. Способен разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	ИПК-2.1. Знает методы концептуального проектирования технологий обеспечения информационной безопасности; ИПК-2.2. Умеет применять методы разработки систем, комплексов, средств и технологий обеспечения информационной безопасности; ИПК-2.3. Владеет навыками разработки систем, комплексов, средств и технологий обеспечения информационной безопасности
ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	ИПК-3.1. Знает: отечественные и международные стандарты информационной безопасности; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; основные методы и средства обеспечения безопасности операционных систем; основные методы и средства обеспечения сетевой безопасности; основные методы и средства обеспечения безопасности в системах управления базами данных. ИПК-3.2. Умеет: обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта

	защиты; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности. ИПК-3.3. Владеет: навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем защиты основных операционных систем.
ПК-15. Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	ИПК-15.1. Знает методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности. ИПК-15.2. Умеет: организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности ИПК-15.3. Владеет методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части/части, формируемой участниками образовательных отношений блока Б1 «Дисциплины (модули)».

Во время освоения дисциплины «Защищенные информационные системы» студентам понадобятся знания, приобретенные ранее в ходе обучения по следующим дисциплинам:

- Методы и средства криптографической защиты информации;
- Стандартизация и сертификация в информационной безопасности;
- Защита информации в автоматизированных системах управления технологическими процессами;
- Защита информации от утечки по техническим каналам;
- Проектирование организационно-распорядительных документов по обеспечению информационной безопасности;
- Программно-аппаратные средства защиты информации.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			3
1	**Аудиторные занятия**	**72**	3
	В том числе:		
1.1	Лекции		3
1.2	Семинарские/практические занятия		3
1.3	Лабораторные занятия	72	3
2	**Самостоятельная работа**	**72**	**3**
3	**Промежуточная аттестация**		**3**
	Экзамен		3
	Итого:	**144**	

3.2 Тематический план изучения дисциплины

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Понятие информационной системы и рассмотрение архитектур применяемых информационных систем	**17**			8		9
2	Раздел 2. Основные аспекты построения ЗИС	**17**			12		9
3	Раздел 3. Описание информационной системы и особенностей ее функционирования	**17**			12		9
4	Раздел 4. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)	**17**			8		9
5	Раздел 5. Определение уровня защищенности данных в информационной системе	**21**			8		9
6	Раздел 6. Описание угроз безопасности информации (модель угроз безопасности информации)	**21**			8		9
7	Раздел 7. Методы выбора системы защиты информации	**17**			8		9

8	Раздел 8. Руководящие документы ФСТЭК России	**17**			8		9
Итого		**144**			**72**		**72**

3.3 Содержание дисциплины

Раздел 1. Понятие информационной системы и рассмотрение архитектур применяемых информационных систем

Понятие информационной системы, основные компоненты информационной системы. Виды информационных систем. Особенности различных архитектур информационных систем. Уровни организации архитектур информационных систем. Особенности распределённых информационных систем.

Раздел 2. Основные аспекты построения ЗИС

Регулирование ответственности нарушений информационной безопасности. Программа информационной безопасности. Контроль деятельности в области безопасности. Модели представления информационной защиты. Формирование требований к системе информационной безопасности. Этапы обеспечения информационной безопасности.

Раздел 3. Описание информационной системы и особенностей ее функционирования

Структура и состав информационной системы. Описание физических, функциональных, технологических и логических взаимосвязей.

Раздел 4. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)

Категория лиц, рассматриваемых и не рассматриваемых в качестве нарушителей. Обобщенные возможности нарушителя. Уточненные возможности нарушителя. Актуальность использования (применения) возможностей нарушителя для построения и реализации атак. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности данных.

Раздел 5. Определение уровня защищенности данных в информационной системе

Определение типа угроз безопасности информации. Определение категории обрабатываемых данных. Определение количества субъектов данных. Определение уровня защищенности данных. Определение класса информационной системы. Оценка степени возможного ущерба. Определение класса защищенности информационной системы.

Раздел 6. Описание угроз безопасности информации (модель угроз безопасности информации)

Определение перечня угроз безопасности информации, возможных с учетом потенциала нарушителя. Определение перечня угроз безопасности информации, возможных с учетом применяемых технологий. Определение исходной защищенности информационной системы. Определение частоты (вероятности) реализации угроз. Определение объема

негативных последствий. Способы реализации угроз безопасности информации. Возможные уязвимости информационной системы.

Раздел 7. Методы выбора системы защиты информации

Классификация методов выбора систем защиты информации. Метод анализа иерархий. Метод парных сравнений альтернатив. Многокритериальный выбор в иерархических структурах с множеством различных альтернатив под критериями. Методы принятия решений, основанные на исследовании операций. Сопоставление угроз и методов и средств их устранения. Игровые стратегии выбора системы защиты информации

Раздел 8. Руководящие документы ФСТЭК России

Требования к защищенности автоматизированных систем. Классы защищённости информационных систем. Аспекты защищённых ИС, фигурирующие в требованиях ФСТЭК. Классификация защищённых информационных систем.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены

3.4.2 Лабораторные занятия

Раздел 1. Понятие информационной системы и рассмотрение архитектур применяемых информационных систем

Лабораторная работа 1. Определение уровня исходной защищённости

Раздел 2. Основные аспекты построения ЗИС

Лабораторная работа 1. Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Лабораторная работа 2. Определение частоты (вероятности) реализации рассматриваемой угрозы

Раздел 3. Описание информационной системы и особенностей ее функционирования

Лабораторная работа 1. Определение коэффициента реализуемости угрозы и возможности реализации

Лабораторная работа 2. Определение типа актуальной угрозы

Раздел 4. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)

Лабораторная работа 1. Создание модели вероятного нарушителя

Раздел 5. Определение уровня защищенности данных в информационной системе

Определение уровня защищенности

Лабораторная работа 1. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Раздел 6. Описание угроз безопасности информации (модель угроз безопасности информации)

Лабораторная работа 1. Составление модели угроз безопасности информационной системы

Раздел 7. Методы выбора системы защиты информации

Лабораторная работа 1. Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах

Раздел 8. Руководящие документы ФСТЭК России

Лабораторная работа 1. Обзор руководящих документов Федеральной службы технического и экспортного контроля (ФСТЭК России)

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный государственный образовательный стандарт высшего образования (уровень магистратуры) по направлению подготовки 10.04.01 Информационная безопасность, утвержденный приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1455.

2. Профессиональные стандарты:

- 06.032 Специалист по безопасности компьютерных систем и сетей. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 533н;
- 06.033 Специалист по защите информации в автоматизированных системах. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 г. № 525н).

4.2 Основная литература

1. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180099 — Режим доступа: для авториз. пользователей.
2. Парфёнов, Ю. П. Средства управления и защиты информационных ресурсов автоматизированных систем : учебное пособие / Ю. П. Парфёнов. — 2-е изд. — Москва : ФЛИНТА, 2022. — 120 с. — ISBN 978-5-9765-5016-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/231707. — Режим доступа: для авториз. пользователей.
3. Программно-аппаратные средства защиты информационных систем : учебное пособие : в 3 частях / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев. — Тамбов : ТГТУ, 2022 — Часть 1 — 2022. — 77 с. — ISBN 978-5-8265-2467-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/355133. — Режим доступа: для авториз. пользователей.

4.3 Дополнительная литература

1. Нестандартные методы защиты информации : учебное пособие / составители В. П. Пашинцев, А. В. Ляхов. — Ставрополь : СКФУ, 2016. — 196 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155239. — Режим доступа: для авториз. пользователей.

2. Щеглов, А. Ю. Математические модели и методы формального проектирования систем защиты информационных систем : учебное пособие / А. Ю. Щеглов, К. А. Щеглов. — Санкт-Петербург : НИУ ИТМО, 2015. — 93 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/70897 — Режим доступа: для авториз. пользователей.

.

4.4 Электронные образовательные ресурсы

ЭОР разрабатывается.

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. OpenOffice: режим доступа: свободный
2. Яндекс.Телемост: режим доступа: свободный.

4.6 Современные профессиональные базы данных и информационные справочные материалы

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.

3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.

4. Библиографическая и реферативная база данных научной периодики «Scopus» - www.scopus.com.

5. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). - http://www.fstec.ru.

6. Портал технического комитета по стандартизации «Защита информации». – http://tk.gost.ru/wps/portal/tk362

7. Информационно-аналитический Интернет-портал ISO27000.ru. – http://www.iso27000.ru/.

.

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран или интерактивная доска) – 1 комплект.

Для проведения практических занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

При подготовке к лабораторным работам следует предварительно проработать теоретический материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия.

При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать правильность выполнения лабораторных работ на всех этапах.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лабораторные и практические работы.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Лабораторные работы проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. Лабораторные работы проводятся по теоретическим и проблемным вопросам ИБ. Лабораторные работы предполагает творческие дискуссии, активный обмен мнениями по поставленным вопросам, заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении лабораторной работы преподаватель выполняет, в основном, функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на лабораторной работе учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др..

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Текущий контроль

Текущий контроль успеваемости студентов осуществляется в процессе проведения лабораторных работ, промежуточных тестов и контрольных работ, подготовленных в рамках самостоятельной работы по темам.

7.3.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен состоит из 2 частей:

- теоретической;
- практической.

а) Примеры типовых заданий для теоретической части экзамена

Задание в открытой форме:

Механизм одобрения для защищенных систем основан на…

Задание на установление правильной последовательности:

Установить последовательность этапов внедрения системы безопасности

1. Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта
2. Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
3. Установка и настройка средств защиты информации
4. Испытания и опытная эксплуатации системы защиты информации

Задание на установление соответствия:

Для информационной ситсемы в составе нескольких защищаемых помещений с числом субъектов ПДн более 100 установите соответствие:

a. Угроза скрытной регистрации вредоносной программой учетных записей администраторов внешний нарушитель с потенциалом не ниже усиленного базового.

b. Угроза хищения аутентификационной информации из временных файлов cookie внешний нарушитель с потенциалом не ниже усиленного базового;

c. Угроза изменения системных и глобальных переменных внутренний нарушитель с потенциалом не ниже усиленного базового;

1 Опасность угрозы низкая

2 Опасность угрозы средняя

3 Опасность угрозы высокая

4 Опасность угрозы приемлемая

б) Примеры типовых заданий для практической части экзамена

Компетентностно-ориентированная задача:

Компания решила перейти на облачные технологии и использовать облачную защищенную информационную систему для хранения конфиденциальных данных о клиентах. Какие меры безопасности необходимо предпринять для защиты информации от несанкционированного доступа, взлома и утечки?