Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.К. АММОСОВА»
Политехнический институт (филиал) ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» в г. Мирном.
Кафедра фундаментальной и прикладной математики

Рабочая программа дисциплины

Б1.В.ДВ.08.01 Теоретические основы компьютерной безопасности

для программы бакалавриата

по направлению подготовки

01.03.02 Прикладная математика и информатика

Профиль подготовки: Математическое моделирование и вычислительная математика

Форма обучения: очная

Автор(ы):
Якушев Илья Анатольевич, к.ф.-м.н., доцент кафедры фундаментальной и прикладной математики, МПТИ (ф)СВФУ, Yakushevilya@mail.ru

РЕКОМЕНДОВАНО Заведующий кафедрой фундаментальной и прикладной математики _____/Гадоев М.Г. протокол №_3__ от «22» февраля 2019 г.	ОДОБРЕНО Заведующий кафедрой фундаментальной и прикладной математики _____/Гадоев М.Г. протокол №_3__ от «22» февраля 2019 г.	ПРОВЕРЕНО Нормоконтроль в составе ОП пройден Ст.диспетчер УМО _____/ Баишева О.Ю. «28» марта 2019 г.
Рекомендовано к утверждению в составе ОП Председатель УМС _____/Константинова Т.П./ протокол УМС № 3 от «29» марта 2019 г.		Эксперт УМС _____/ Егорова М.В. «29» марта 2019 г.

Мирный 2019

АННОТАЦИЯ
к рабочей программе дисциплины
Б1.В.ДВ.08.01 Теоретические основы компьютерной безопасности
Трудоемкость 3 з.е.

1.1. Цель освоения н краткое содержание дисциплины

Цель освоения: раскрыть содержание основных понятий и формальных моделей обеспечения безопасности компьютерных систем (моделей компьютерной безопасности).

Краткое содержание дисциплины: История развития теории и практики обеспечения компьютерной безопасности. Понятие и составляющие компьютерной безопасности. Систематика методов и механизмов обеспечения компьютерной безопасности. Понятие угроз безопасности, основы их классификации (каталогизации). Методы и проблемы оценивания угроз безопасности. Понятие политики безопасности в компьютерных системах и неформализованное выражение в моделях безопасности.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Планируемые результаты освоения программы (код и содержание компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения по дисциплине	Оценочные средства
ПК	ПК-2 Способность понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии.	ПК-2.1. Знает основные методы решения прикладных задач, современные методы информационных технологий. ПК-2.2. Умеет корректно оформить результаты научного труда в соответствии с современными требованиями. ПК-2.3. Имеет практический опыт использования сети Интернет, аннотирования, реферирования, библиографического разыскания и описания, опыт работы с научными источниками	**Знать:** структуру и правила оформления исследовательской и проектной работы. **Уметь:** формулировать тему исследовательской и проектной работы, доказывать ее актуальность; составлять индивидуальный план исследовательской и проектной работы; выделять объект и предмет исследовательской и проектной	Выполнение практических заданий, тест, устный опрос

			работы; определять цель и задачи исследовательской и проектной работы. **Владеть** понятиями: библиография, курсовой проект, дипломный проект, гипотеза исследования, моделирование, обобщение, объект исследования, предмет исследования,	
ПК	ПК-7. Способен анализировать требования к программному обеспечению и, внедрять методы обработки и анализа данных, включая технологии искусственного интеллекта, при разработке информационных систем цифровой экономики.	ПК-7.1. Анализирует требования к программному обеспечению ПК-7.2. Проектирует структуры данных и программные интерфейсы, разрабатывает архитектуру программного обеспечения	**Знать** компоненты архитектуры информационных технологий, структуру, состав, задачи и значение ИТинфраструктуры предприятия классификацию и характеристики аппаратных и программных средств основные процессы ИТ-инфраструктуры. **Уметь** осуществлять проектирование и разработку архитектуры программной системы, устанавливать программное обеспечение. **Владеть** средствами программного обеспечения анализа и количественного моделирования	Выполнение практических заданий, тест, устный опрос

			систем управления.	

1.3. Место дисциплины в структуре ОПОП

Индекс	Наименование дисциплины (модуля), практики	Семестр изучения	Индексы и наименования учебных дисциплин (модулей), практик	
			на которые опирается содержание данной дисциплины (модуля)	для которых содержание данной дисциплины (модуля) выступает опорой
Б1.В.ДВ.08.01	Теоретические основы компьютерной безопасности	8	Б1.О.35. Системы программирования	-

1.4. Язык преподавания: русский

2. **Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Выписка из учебного плана:

Код и название дисциплины по учебному плану	Б1.В.ДВ.08.01 Теоретические основы компьютерной безопасности	
Курс изучения	4	
Семестр(ы) изучения	8	
Форма промежуточной аттестации (зачет/экзамен)	Зачет	
Курсовой проект/ курсовая работа (указать вид работы при наличии в учебном плане), семестр выполнения	-	
Трудоемкость (в ЗЕТ)	3	
Трудоемкость (в часах) (сумма строк №1,2,3), в т.ч.:	108	
№1. Контактная работа обучающихся с преподавателем (КР), в часах:	Объем аудиторной работы, в часах	Вт.ч. с применением ДОТ или ЭО, в часах
Объем работы (в часах) (1.1.+1.2.+1.3.):	57	-
1.1. Занятия лекционного типа (лекции)	26	-
1.2. Занятия семинарского типа, всего, в т.ч.:	26	-
- семинары (практические занятия, коллоквиумы и т.п.)	26	-
- лабораторные работы	-	-
- практикумы	-	-
1.3. КСР (контроль самостоятельной работы, консультации)	5	-
№2. Самостоятельная работа обучающихся (СРС) (в часах)	51	
№3. Количество часов на экзамен (при наличии экзамена в учебном плане)	-	

3.Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

3.1. Распределение часов по темам и видам учебных занятий

Тема	Всего часов	Контактная работа, в часах									Часы СРС
		Лекции	из них с применением ЭО и ДОТ	Семинары (практические занятия, коллоквиумы)	из них с применением ЭО и ДОТ	Лабораторные работы	из них с применением ЭО и ДОТ	Практикумы	из них с применением ЭО и ДОТ	КСР (консультации)	
Исходные положения теории компьютерной безопасности	36	10		10						1	15
Модели безопасности компьютерных систем	34	8		8						2	16
Методы анализа и оценки защищенности компьютерных систем	38	8		8						2	20
Всего часов	**108**	**26**		**26**		**-**	**-**	**-**	**-**	**5**	**51**

3.2. Содержание тем программы дисциплины

Тема 1. Исходные положения теории компьютерной безопасности

Содержание и основные понятия компьютерной безопасности

История развития теории и практики обеспечения компьютерной безопасности. Понятия "информационная безопасность" и компьютерная безопасность. Безопасность информации в компьютерных системах и ее составляющие – конфиденциальность, целостность и правомерная доступность (сохранность) информации. Субъекты и объекты безопасности. Угрозы безопасности. Нарушители безопасности. Общие принципы обеспечения компьютерной безопасности. Систематика методов и механизмов обеспечения компьютерной безопасности. Методы и механизмы, непосредственно обеспечивающие конфиденциальность, целостность и доступность информации — разграничение доступа к данным, контроль, управления информационной структурой данных, установление и контроль ограничений целостности данных, шифрование данных, механизмы ЭЦП данных в процессах их передачи и хранения, защита/удаление остаточной информации на носителях данных и в освобождаемых областях оперативной памяти. Методы и механизмы общеархитектурного характера — идентификация/аутентификация пользователей, устройств, данных, управление памятью, потоками, изоляция процессов, управление транзакциями. Методы и механизмы инфраструктурного характера — управление (контроль) конфигурацией, управление сеансами, управление удаленным доступом с рабочих станций, управление сетевым соединениями, управление инфраструктурой сертификатов криптоключей. Методы и механизмы обеспечивающего (профилактирующего) характера — протоколирование и

аудит событий, резервирование данных, журнализация процессов изменения данных, профилактика, учет и контроль использования носителей данных, нормативноорганизационная регламентация использования КС, обучение, нормативно-административное побуждение и принуждение пользователей по вопросам информационной безопасности КС.

Угрозы безопасности в компьютерных системах

Понятие угрозы. Угрозы безопасности информации в компьютерных системах. Понятия "идентификация", "аутентификация", "авторизация", "спецификация", "классификация", "категорирование" и "каталогизация". Классификационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации — критерии выделения и таксономия классов (алгебраическая полнота в операциях пересечения и объединения классов). Примеры и проблемы теоретического обоснования каталогов угроз по зарубежным, отечественным и международным стандартам. Идентификация и спецификация (описание) угроз — выявление угрозы определенного типа и присвоение ей уникального идентификатора, определение и описания источника 8 (природы) угрозы, активов/объектов, подверженных воздействию угрозы, способов и особенностей реализации/осуществления. Общая схема оценивания угроз — оценка [вероятности] реализации угрозы и оценка ущерба от реализации угрозы. Оценка рисков, методы и шкалы оценки. Методы экспертной оценки вероятности реализации и/или степени опасности угроз. Человеческий фактор в угрозах безопасности и модель нарушителя информационной безопасности.

Политика и модели безопасности в компьютерных системах

Понятие политики безопасности. Модель безопасности как формализованное выражение политики безопасности. Модель безопасности как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС. Составляющие модели безопасности — модель (формализация) компьютерной системы в аспекте безопасности информации, критерии, формализованные правила, алгоритмы, механизмы безопасного функционирования КС. Класс моделей конечных состояний. Компьютерная система как автомат (процесс) с дискретным временем функционирования. Теоретико-множественная субъектно-объектная формализация (модель) компьютерной системы. Понятие субъекта и объекта, потока информации и доступа субъекта к объекту, методов и прав доступа, разграничения доступа. Основные типы политик безопасности — дискреционная, мандатная, тематическая, ролевая, временна́я, маршрутная. Программно-техническая структура компьютерной системы в контексте безопасности. Понятие и функции монитора (ядра) безопасности. Требования к монитору безопасности. Монитор безопасности объектов (монитор ссылок) и монитор безопасности субъектов (монитор приложений). Гарантирование выполнения политики безопасности. Тождественность объектов и тождественность субъектов доступа (неизменность свойств). Модель и теоремы гарантирования безопасности (по Щербакову). Изолированная программная среда.

Тема 2. Модели безопасности компьютерных систем

Модели безопасности на основе дискреционной политики

Общая характеристика политики дискреционного доступа. Тройки доступа: субъектоперация-объект. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа. Пятимерное пространство Хартсона как пример выражения дискреционного разграничения доступа на языке реляционной алгебры. Модели разграничения доступа на основе матрицы доступа. Принудительный и добровольный принцип управления доступом. Администраторы системы и владельцы объектов. Привилегии и предоставление (распространение) прав доступа. Способы организации информационной структуры матрицы доступа — централизованная структура (системные таблицы доступа в реляционных СУБД, биты доступа в ОС UNIX)

и децентрализованная структура (списки доступа объектов в ОС Windows). Модель распространения прав доступа Харисона-Руззо-Ульмана. Примитивные операции и команды изменения матрицы доступа. Монотонные, монооперационные и одноусловные системы. Теорема безопасности Харисона-Руззо-Ульмана для монооперационных систем и в общем случае. Троянские программы. Сценарий атаки троянской программой в нотации модели Харисона-Руззо-Ульмана. Модель типизованной матрицы доступа как расширение модели Харисона-Руззо-Ульмана и способ разрешения проблемы троянских программ. Типы субъектов и объектов. Родительские и дочерние типы. Граф отношений (порождений) наследственности. Теорема безопасности для ацикличных реализаций систем на основе типизованной матрицы доступа. Теоретико-графовая модель TAKE-GRANT для исследования распространения прав доступа в системах с добровольным управлением доступом. Специфичные права субъектов доступа take и grant. Граф доступа. Примитивные операции (команды), изменяющие состояние графа доступа. tg-связность вершин графа доступа, "острова" и "мосты" в графе доступа. Условия и теорема возможности санкционированного получения субъектом прав доступа на какой-либо объект. Условия и теорема возможности несанкционированного получения субъектом прав доступа на какой-либо объект ("похищения" прав доступа). Расширенная (extended) модель TAKE-GRANT. Неявные (вероятностные) каналы утечки информации и "мнимые" дуги в графе доступов. Примитивные (элементарные) команды преобразования графа доступов для генерации мнимых дуг (команды де-факто). Графовые пути возможностей утечки информации по графу доступа.

Модели безопасности на основе мандатной политики

Общая характеристика политики мандатного (полномочного) доступа. Парадигма градуированного доверия пользователям (субъектам доступа) и градуированной степени конфиденциальности данных (объектов доступа). Уровни безопасности субъектов и объектов доступа. Правила безопасного мандатного доступа — запрет чтения вверх (NRU) и запрет записи вниз (NWD). Рефрексивность, антисимметричность и транзитивность отношений доступа. Функция уровня безопасности субъектов и объектов доступа. Решетка уровней безопасности. Классы безопасных информационных потоков и матрица доступа. Модель безопасности Белла-ЛаПадулы. Критерий безопасного состояния системы. Функция перехода системы из одного состояния в другое. Основная теорема безопасности (теорема безопасности Белла-ЛаПадулы). Недостатки и "абстрактность" систем на основе модели Белла-ЛаПадулы (Z-системы и др.). Расширения модели Белла-ЛаПадулы. Безопасная функция перехода МакЛина и теорема безопасности МакЛина, разрешение проблемы Z-системы. Уполномоченные (доверенные) субъекты и авторизованная функция перехода МакЛина. Групповые субъекты доступа. Модель совместного доступа МакЛина. Правила безопасного доступа NRU и NWD для групповых субъектов. Другие расширения модели Белла-ЛаПадулы. Модель Low-WaterMark.

Модели безопасности на основе тематической политики

Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств. Критерии безопасности информационных потоков в системах тематического разграничения доступа. Тематические решетки на основе классификационных множеств. Решетка подмножеств множества тематических рубрик при дескрипторной классификации. Тематическая решетка на корневом дереве рубрикатора при монорубрицированной иерархической классификации и ее изоморфный вариант в виде решетки листовых подмножеств. Тематические мультирубрики при мультирубрицированной иерархической классификации субъектов и объектов доступа. Алгебра (решетка) мультирубрик. Отношения доминирования мультирубрик, операции (механизмы) наименьшей верхней и наибольшей нижней границ мультирубрик. Модель тематико-иерархического разграничения доступа в системах с мультирубрицированной

тематической классификацией субъектов и объектов доступа.

Модели безопасности на основе ролевой политики

Общая характеристика политики ролевого (типизованного) доступа. Роль как типовой субъект доступа (функционально обособленное агрегирование прав доступа и полномочий выполнения процедур над данными). Две фазы организации ролевого доступа — создание ролей как типовых субъектов доступа с наделением их правами (полномочиями) доступа на основе дискреционной, мандатной, тематической или иной политики безопасности и назначение ролей пользователям. Сеансовый характер функционирования компьютерной системы с ролевым доступом. Сеансовая авторизация пользователя с одной или группой назначенных ему в системе ролей и доступ к объектам системы в соответствующей (соответствующих) роли (ролях). Разновидности ролевых систем по отношениям ролей, принципам назначения ролей пользователям и сеансовой авторизации пользователей с назначенными ролями. Системы с иерархической организацией ролей, с взаимоисключающими в системе ролями (статическое распределение обязанностей), с взаимоисключающими в рамках одного сеанса ролями (динамическое распределение обязанностей) и др. Способы наделения правами доступа ролей (ролевых субъектов доступа) в системах с иерархической организацией ролей. Модель индивидуально-группового доступа. Отличия рабочих групп от ролей. Теоретикомножественная формализация индивидуально-группового доступа. MMS-модель (military message system) Лендвера-МакЛина как пример сочетания дискреционной, мандатной и ролевой политики безопасности.

Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости

Понятие и общая характеристика скрытых каналов утечки информации. Скрытые каналы "по памяти", скрытые каналы "по времени", статистические скрытые каналы ("по статистике"). Примеры реализации скрытых каналов утечки информации. Понятие емкости (пропускной способности) скрытых каналов передачи данных. Автоматная модель информационного невлияния Гогена-Мессигера. Функция истории вводов и функция очищения. Модель Гогена-Мессигера как теоретико-методологическая база интерфейса защищенных КС в аспекте устранения (перекрытия) скрытых каналов утечки информации "по времени". Теоретико-вероятностная трактовка информационного потока (по К.Шеннону). Модели информационной невыводимости и информационного невлияния как теоретикометодологическая основа анализа (выявления) и перекрытия скрытых каналов "по памяти" и "по статистике". Теоретико-вероятностная трактовка автоматной модели Гогена-Мессигера. Технологии представлений (views) в реляционных СУБД как пример реализации подходов информационной невыводимости и информационного невлияния.

Модели и механизмы обеспечения целостности данных

Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостности данных. Дискреционная модель обеспечения целостности данных Кларка-Вильсона. Объекты, требующие контроля целостности (constrained data items), процедуры проверки целостности (integrity verification procedures), корректно сформированные транзакции (не нарушающие ограничения целостности), тройки "субъект-транзакция-объект". Мандатная модель К.Биба. Уровни целостности данных. Уровни доверия пользователям. Правила мандатного доступа, не нарушающие целостность данных (запрет "чтения вниз", запрет "записи вверх") как инверсия правилам мандатного доступа, не нарушающим конфиденциальность данных (в модели Белла-Лападулы). Проблемы и разновидности совместимости в практической реализации моделей БеллаЛаПадулы и К.Биба: на основе двух разных решеток безопасности (отдельных систем уровней конфиденциальности и целостности), на основе одной общей решетки, но с двумя отдельными метками для объектов и субъектов (на чтение, на запись). Транзакционная парадигма коллективной (одновременной) обработки данных в клиентсерверных

системах. Принципы "атомарности" (неделимости), "изоляции" транзакций. Нарушения целостности, возникающие при совместной обработке данных, одновременном (параллельном) выполнении транзакций пользователей. Понятие и виды "грязных" (dirty) данных – "грязное чтение" (dirty read), "потерянные изменения" (lost update) и "неповторяющееся чтение" (unrepeatable read). Протоколы выполнения и фиксации транзакций. Протоколы, основанные на "захватах" блокировках объектов. Двухфазной протокол выполнения и фиксации транзакций ("пессимистичный" режим выполнения транзакций). Тупики (Deadlock), их обнаружение и разрушение. Механизмы изоляции транзакций, основанные на временных метках объектов ("оптимистичный" режим выполнения транзакций).

Методы и технологии обеспечения доступности (сохранности) данных

Резервирование, архивирование и журнализация данных. Организационные, технологические и программно-технические принципы политики резервирования и архивирования БД. Оперативное сохранение (журнализация) изменений данных. Восстановление данных из архивной копии и по журналу изменений данных. Синхронная и асинхронная журнализация. Полное и инкрементное сохранение измененных данных. Сценарии архивирования/журнализации. Системы реального времени. "Горячее" резервирование. Главный/резервный серверы. "Прозрачность" для приложений. Автоматическое переключение серверов, "поднятие" "упавшего" сервера. Системы репликации данных. Обеспечение непрерывности согласованного состояния данных, синхронная и асинхронная репликации. Программно-техническая структура систем репликации данных. Обеспечение непрерывности согласованного состояния структуры данных, системы с "главной" и частичными репликами.

Политика и модели безопасности в распределенных компьютерных системах

Понятие "распределенности" компьютерных систем в аспекте безопасности. Дополнительные аспекты политики безопасности в распределенных компьютерных системах. Структура распределенных компьютерных систем в аспекте политики безопасности. Понятие локального сегмента и удаленного доступа субъекта к объектам. Локальная и общесетевая (общесистемная) политика безопасности. Субъект (субъекты) реализации политики безопасности в распределенных компьютерных системах. Модель безопасности Варахаратжана. Фазы доступа. Зональная политика безопасности и ее теоретико-множественное формализация (модель). Внутризональные и межзональные (общесистемные) аспекты политики безопасности. Доверительные отношения зон безопасности (локальных сегментов с обособленным монитором безопасности). Реализация зонально-межзональных принципов политики безопасности в распределенных компьютерных системах на примере доменно-групповой архитектуры сетей на основе ОС Windows.

Тема 3. Методы анализа и оценки защищенности компьютерных систем

Методы, критерии и шкалы оценки защищенности (безопасности) компьютерных систем

Понятие измерения величин и оценки объектов как отображения множеств с отношениями. Процесс измерения (оценки) и шкала измерения (оценки). Точные измерения и измерения с погрешностями. Типы шкал (шкалирования) – номинальные шкалы, порядковые (ранговые) шкалы, шкалы интервалов, шкалы отношений, шкалы разностей и абсолютные шкалы. Многомерное оценивание сложных объектов и его целевые разновидности – определение сравнительного предпочтения объектов, определение сходства и различия объектов, типизация (классификация и группирование) объектов. Матрица "Объекты-признаки". Снижение размерности пространства признаков путем их агрегирования в оценочные факторы для определения предпочтений. Расстояния в пространстве признаков для определения схожести объектов. Сгущения в пространстве признаков и выделение классов (группирование) объектов. Оценка защищенности (безопасности) компьютерных систем как задача многомерного шкалирования свойств КС в аспекте безопасности. Иерархический (древовидный) характер системы критериев

анализа КС (параметров, свойств, функций), обеспечивающих составляющие безопасности (конфиденциальность, целостность и доступность информации). Номинальный или иной (порядковый, абсолютный и т.д.) характер шкалирования параметров, свойств и функций безопасности КС. Безопасность (защищенность) компьютерных систем как обобщенный (абстрактный) фактор, агрегирующий результаты оценки параметров, свойств и функций безопасности. Порядковое (ранговое) шкалирование компьютерных систем в аспекте безопасности на основе группирования (классификации) в пространстве шкалирования первичных факторов оценки. Примеры многомерных номинально-ранговых систем оценки защищенности компьютерных систем, закрепленные в стандартах безопасности.

Теоретико-графовые модели комплексной оценки защищенности компьютерных систем

Теоретико-графовая модель систем защиты с полным перекрытием [угроз] на основе двудольного графа "Угрозы-Объекты". Модель Клементса. Разновидности теоретико-графового подхода к моделированию систем комплексной оценки защищенности в виде трехдольных ("Угрозы-Средства/МерыЗащиты-Объекты" и взвешенных графов (взвешенность вершин-объектов по ценности, взвешенность вершин "Средств/мер защиты" по стоимости осуществления, взвешенность дуг "угрозы-объекты" по вероятности реализации угроз, взвешенность дуг "средства/меры_защиты-угрозы" по степени снижения вероятности реализации угроз). Векторно-матричное представление взвешенного графа "Угрозы-Средства/МерыЗащиты-Объекты". Технико-экономическое обоснование (анализ) систем защиты. Критерий эффективности как отношение величины снижения потенциального ущерба от реализации угроз при выбранных средствах/мерах защиты к сумме стоимости объектов защиты и стоимости задействования средств/мер защиты. Выражения для вычисления критерия технико-экономической эффективности на основе векторно-матричного представления графа "УгрозыСредства/МерыЗащиты-Объекты". Тактико-техническое обоснование систем защиты. Критерий эффективности как вероятности преодоления системы защиты и его вычисление на основе взвешенного графа "Угрозы-Средства/МерыЗащиты-Объекты". Проблемы методов и шкал оценки ценности (стоимости) объектов, стоимости защитных мер, вероятности реализации угроз. Ранговые шкалы оценки рисков от реализации угроз безопасности.

Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа

Проблемы проектирования (синтеза) и анализа систем индивидуально-группового доступа. Теоретико-графовая формализация (модель) систем индивидуально-группового назначения пользователям (субъектам доступа) прав доступа к иерархически организованным ресурсам (объектам доступа). Матричное выражение графа индивидуально-групповых назначений доступа. Матричные соотношения для вычисления итоговых прав доступа. Коэффициенты дублирования прав доступа, превышения и недостатка прав доступа как количественные параметры оптимизации систем индивидуально-группового доступа и их матричные выражения. Методы проектирования системы рабочих групп пользователей – "сверху" (по организационно-функциональной структуре коллектива пользователей) и "снизу" (по схожести индивидуальных потребностей пользователей в правах доступа к объектам). Выражение для вычисления меры близости пользователей по требуемым правам доступа. Мера близости рабочих групп пользователей по составу пользователей и итоговым правам доступа с учетом вхождения одних рабочих групп в другие и иерархической организации объектов доступа как параметр оптимизации систем индивидуально-группового доступа.

3.3. Формы и методы проведения занятий, применяемые учебные технологии

При проведении занятий применяется игровое проектирование, компьютерная симуляция, дискуссия.

4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине:

1. Подготовка к практическим занятиям.
2. Самостоятельное изучение отдельных вопросов в соответствии со структурой дисциплины, составление конспектов.
3. Самостоятельное выполнение практических работ.
4. Подготовка к тестированию, аудиторной контрольной работе.
5. Выполнение домашних заданий.
6. Подготовка к промежуточной аттестации.

Содержание СРС

№	Наименование раздела (темы) дисциплины	Вид СРС	Трудо-емкость (в часах)	Формы и методы контроля
1.	Исходные положения теории компьютерной безопасности	Отработка доказательств теорем и решение задач по моделям дискреционного, мандатного, тематического и ролевого доступа.	15	Оценка по БРС
2.	Модели безопасности компьютерных систем		16	Оценка по БРС
3.	Методы анализа и оценки защищенности компьютерных систем	Решение задач по моделям комплексной оценки защищенности КС, по методам анализа и оптимизации систем индивидуально-группового назначения прав доступа к иерархически организованным объектам. Изучение и анализ классификационных схем (каталогов) угроз по стандартам безопасности. Изучение и анализ систем номинально-ранговой оценки защищенности КС, закрепленных в Руководящих документах Гостехкомиссии (ФСТЭК) России по защите от НСД к информации.	20	Оценка по БРС
	Всего часов		**51**	

5. Методические указания для обучающихся по освоению дисциплины

Балльно-рейтинговая система по дисциплине

Рейтинговый регламент по дисциплине:

Вид выполняемой учебной работы (контролирующие мероприятия)	Количество баллов (min)	Количество баллов (max)
Функциональное и системное наполнение пакета «Теоретические основы компьютерной безопасности»	12	20
Встроенный программный язык	12	20
Использование основных объектов конфигурации. Работа с документами	12	20
Отчеты в «Теоретические основы компьютерной безопасности»	12	20
Разработка и создание интерфейса	12	20
Количество баллов для получения зачета (min-max)	**60**	**100**

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1. Показатели, критерии и шкала оценивания

Коды оцениваемых компетенций	Показатель оценивания (дескриптор) (по П.1.2.РПД)	Уровни освоения	Критерий оценивания	Оценка
ПК-2, ПК-7	См. п. 1.2	Высокий	Освоены все компетенции. Студент глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.	отлично

		Базовый	Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.	хорошо
		Мини-мальный	Студент имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.	удовлетво-рительно
		Не освоены	Студент не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.	неудовлетво-рительно

6.2. Типовые контрольные задания (вопросы) для промежуточной аттестации

Коды оцениваемых компетенций	Оцениваемый показатель (ЗУВ)	Тема	Образец типового (тестового или практического) задания (вопроса)
ПК-2, ПК-7	*Знать:* методы администрирования и контроля; возможности платформ, средств и систем администрирования; способы проектирования компонентов информационных систем; функционирование основных протоколов и сервисов Интернета; выбирать средства обеспечения информационной безопасности информационной системы современного предприятия; *Уметь:* проектировать, устанавливать и настраивать службы безопасности, организации доступа, именования и адресации; активизировать, конфигурировать и контролировать работу стандартных сервисов сетевых операционных систем; анализировать состояния и функционирования систем и информационных потоков; использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов. *Владеть:* самостоятельным проектированием, развертыванием и администрированием информационных систем;	Исходные положения теории компьютерной безопасности	1. История теории и практики компьютерной безопасности 2. Структура понятия компьютерная безопасность и основные направления ее обеспечения 3. Понятие защищенности (безопасности) компьютерной информации. Конфиденциальность, целостность и доступность информации. 4. Понятие угроз безопасности компьютерной информации и их классификация 5. Таксонометрия угроз безопасности и изъянов (брешей) систем защиты. ГОСТ Р 51275-99. 6. Человеческий фактор и модель нарушителя безопасности информации 7. Субъектно-объектная модель компьютерной системы. Понятие потока, доступа и правил разграничения доступа. Основные типы политик разграничения доступа. 8. Монитор безопасности КС и гарантирование выполнение политики безопасности. Изолированная программная среда. 9. Дискреционные модели безопасности компьютерных систем. Пятимерное пространство Хартсона 17 10. Модели безопасности на основе матрицы доступа. Способы организации матрицы доступа и управления доступом в компьютерных системах 11. Дискреционные модели распространения прав доступа. Модель и теоремы безопасности Харрисона-Руззо-Ульмана. 12. Модель типизованной матрицы доступа. 13. Модель TAKE-GRANT. 14. Расширенная модель TAKE-GRANT. 15. Основы политики мандатного доступа. Решетка
		Модели безопасности компьютерных систем	
		Методы анализа и оценки защищенности компьютерных систем	

	анализом, управлением, и контролем состояния работающих информационных систем; разработкой собственных методов решения в области информационных систем и сетевых коммуникаций; основными программно-аппаратными средствами и методами защиты компьютерных систем.		безопасности. 16. Модель Белла-ЛаПадулы и основная теорема безопасности 17. Основные расширения модели Белла-ЛаПадулы. 18. Общая характеристика политики тематического разграничения доступа. 19. Решетки в моделях тематического разграничения доступа. Решетка мультирубрик на иерархических рубрикаторах. 20. Скрытые каналы утечки информации и теоретико-информационные модели безопасности. Технологии "представлений" и "разрешенных процедур". 21. Модели ролевого доступа. Иерархические системы ролей. Принципы наделения ролей полномочиями. 22. Политика и зональная модель безопасности в распределенных КС. 23. Модели обеспечения целостности. Дискреционная модель Кларка-Вильсона. 24. Модели обеспечения целостности. Мандатная модель Кена Биба. 25. Объединение мандатных моделей Белла-ЛаПадулы и Кена Биба. 26. Обеспечение целостности данных мониторами транзакций в клиент-серверных системах 27. Методы, критерии и шкалы оценки эмпирических объектов. 28. Системы многомерного шкалирования защищенности компьютерных систем. 29. Теоретико-графовые модели комплексной оценки защищенности КС. Технико-экономическое обоснование систем обеспечения безопасности. 30. Теоретико-графовые модели комплексной оценки защищенности КС. Тактико-техническое обоснование систем обеспечения безопасности. 31. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически

			организованным информационным ресурсам. Итоговые права доступа. 32. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Количественные параметры систем индивидуально-группового доступа.

6.3. Методические материалы, определяющие процедуру оценивания

Промежуточный контроль является заключительным занятием по основным разделам программы в виде контрольной работы в виде практических задач.

Итоговый контроль проводится в виде зачета. На зачете студенты получают билет, состоящий из теоретических вопросов и практических заданий.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№	Автор, название, место издания, издательство, год издания учебной литературы, вид и характеристика иных информационных ресурсов	Наличие грифа, вид грифа	Кол-во экземпляров в библиотеке МПТИ (ф) СВФУ	Электронные издания: точка доступа к ресурсу (наименование ЭБС, ЭБ СВФУ)
Основная литература				
1	Шаньгин В.Ф. Комплексная защита информации в корпоративных системах учебное пособие М.: Форум:Инфра-м 2013	УМО	18	
2	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. - М.: Форум:Инфра-м, 2013	МО	18	
3				
Дополнительная литература				
1	Могилев А.В. Практикум по информатике. Академия, 2008	МО	15	
2	Чуянов А.Г. Обеспечение информационной безопасности в компьютерных системах учебное пособие Омск : Омская академия МВД России 2012			http://www.iprbookshop.ru/36015.html
3	Башлы П.Н, Информационная безопасность и защита информации учебное пособие М.: Евразийский открытый институт 2012			http://www.iprbookshop.ru/10677.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее сетъ-Интернет), необходимых для освоения дисциплины

1. ЭБС «Университетская библиотека онлайн» www.biblioclub.ru
2. ЭБС IPRbooks http://www.iprbookshop.ru/
3. Научная электронная библиотека http://elibrary.ru

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия проводятся в компьютерном классе, оборудованным ПК, интерактивной доской, специальным оборудованием для создания и воспроизведения мультимедиа.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечении и информационных справочных систем

10.1. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

- использование на занятиях электронных изданий;
- использование специализированных и офисных программ.

10.2. Перечень программного обеспечения

Пакет локальных офисных программ для работы с документами (лицензия № 62235736 от 06.08.2013 г.) АО «СофтЛайн Интернет Трейд» на право использование программ для ЭВМ: Microsoft (Windows, Office).

10.3. Перечень информационных справочных систем

Консультант, Гарант

ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.ДВ.08.01 Теоретические основы компьютерной безопасности

Учебный год	Внесенные изменения	Преподаватель (ФИО)	Протокол заседания выпускающей кафедры (дата, номер),ФИО зав. кафедрой, ПОДПИСЬ
2021-2022г.	Внесено изменение в формулировке компетенции ОПК-4	Якушев И.А.	28.09.2021г. №2. Гадоев М.Г.
2022-2023 г.	Изменения в компетенциях	Якушев И.А	13.09.2022г. №1. Гадоев М.Г