Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

УТВЕРЖДАЮ
И.о. проректора
А.В. Троицкий
«___»_____2023 г.

Троицкий Александр Витальевич
Подписано цифровой подписью: Троицкий Александр Витальевич

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ
«ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 09.04.03 Прикладная информатика

Профиль: Моделирование и проектирование информационных систем

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Журавлев С.И. Рабочая программа дисциплины: Теоретические основы компьютерной безопасности. – Королев МО: «Технологический Университет», 2023.

Рецензент: **к.т.н., доцент Соляной В. НСазонов С.Ю.**

Рабочая программа составлена в соответствии с требованиями федерального Государственного образовательного стандарта высшего профессионального образования по направлению подготовки магистров 09.04.03 «Прикладная информатика» и Учебного плана, утвержденного Ученым советом Университета. Протокол №9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Сазонов С.Ю. к.т.н., доцент			
Год утверждения (переутверждения)	2023			
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП к.т.н., доцент Раев О.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023			
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является:

1. Сформировать у студентов базовые знания и практические навыки защиты информации в компьютерных системах.

2. Освоение студентами теоретических основ, технологий и механизмов защиты компьютерных систем.

В процессе обучения студент приобретает и совершенствует следующие **компетенции**:

- ПК-1 Способность применять современные методы и инструментальные средства прикладной информатики для автоматизации решения прикладных задач различных классов и создания ИС;
- ПК-5 Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.

Основными **задачами** дисциплины являются:

1. ознакомление студентов с теоретическими основами и нормативной базой, применяемых для построения защищенных информационных систем;
2. формирование у студентов базовых знаний в области технологий и механизмов защиты информации, применяемых в компьютерных системах;
3. привитие студентам навыков практической работы с программно-аппаратными средствами защиты информации;
4. подготовка студентов применять стандарты по оценке информационной защищённости при анализе и проектировании защищённых компьютерных систем.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- Имеет понятие о методах и инструментальных средствах прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС
- Понимает передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.

Необходимые умения:

- Использует методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС
- Использует передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.

Трудовые действия:

- Применяет методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС
- Применяет передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки магистров по направлению подготовки 09.04.03 «Прикладная информатика».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на компетенциях, освоенных в курсе «Компьютерное моделирование бизнес процессов» (ПК-3, 6, 7), и служит основой изучения курса «Защищенные ИС».

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для обучающихся очной формы составляет 2 зачетные единицы, 72 часа.

Таблица1

Виды занятий	**Всего часов**	**Семестр …..**	**Семестр 3**	**Семестр …**	**Семестр …**
Общая трудоемкость	**72**		**72**		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**24**		**24**		
Лекции (Л)	8		8		
Практические занятия (ПЗ)	16		16		
Лабораторные работы (ЛР)					
Практическая подготовка	-		-		
Самостоятельная работа	**48**		**48**		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа	+		+		
Текущий контроль знаний	-		-		
Вид итогового контроля	**экзамен**		**экзамен**		

4. Содержание дисциплины
4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час.	Практические занятия, час.	Занятия в интерактивной форме	Практическая подготовка	Код компетенций
Раздел 1. Концептуально-теоретические основы компьютерной безопасности					
Тема 1. Введение. Основные понятия теории компьютерной безопасности	1	1	1	-	ПК-1, ПК-5
Тема 2. Анализ угроз информационной безопасности для компьютерных систем	1	2		-	ПК-1, ПК-5
Тема 3. Основные уровни защиты информации в компьютерных системах	1	2	1	-	ПК-1, ПК-5
Тема 4. Основные положения формальной теории защиты информации	1	2	1	-	ПК-1, ПК-5
Тема 5. Формальные модели безопасности	1	2		-	ПК-1, ПК-5
Тема 6. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам	1	2	1	-	ПК-1, ПК-5
Тема 7. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации	0,5	2	1	-	ПК-1, ПК-5
Раздел 2. Прикладные основы теории компьютерной безопасности					
Тема № 8. Методология обследования и проектирования защищенных информационных (автоматизированных) систем	0,5	1	1	-	ПК-1, ПК-5
Тема № 9. Общие сведения о стандартах в области информационной безопасности. Стандарт «Критерии оценки доверенных компьютерных систем»/ TCSEC («Оранжевая книга»). Общие критерии оценки безопасности информационных технологий («Common Criteria»)	0,5	1		-	ПК-1, ПК-5
Тема № 10. Концепция защиты СВТ и АС от НСД в соответствии с руководящими документами Гостехкомиссии и нормативно-методическими документами ФСТЭК России	0,5	1		-	ПК-1, ПК-5
Итого:	**8**	**16**	**12**	**-**	

4.2. Содержание тем дисциплины

Раздел 1. Концептуально-теоретические основы компьютерной безопасности

Тема 1. Введение. Основные понятия теории компьютерной безопасности

Введение. Место и роль дисциплины в процессе подготовки магистра, связь с другими дисциплинами. Структура и содержание дисциплины. Виды занятий и контрольных мероприятий. Рекомендуемая литература.

Актуальность проблемы обеспечения информационной безопасности (ИБ) в компьютерных системах. Современная постановка целей и задач по обеспечению компьютерной безопасности (переход к тотальной защите и интенсивным мерам). Основные термины и определения в области ИБ компьютерных систем и сетей.

Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Факты, свидетельствующие о способах злоупотребления информацией, циркулирующей в компьютерных системах.

Тема 2. Анализ угроз информационной безопасности для компьютерных систем

Проблемы безопасности компьютерных систем (сетей). Понятие угрозы. Цели злоумышленников, осуществляющих основные атаки.

Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. Уязвимости АС, возможные атаки на них. Особенности построения систем обнаружения атак (СОА) в АС. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).

Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.

Причины возникновения угроз безопасности информации. Отличительные особенности угроз корпоративным и локально-вычислительным сетям.

Тема 3. Основные уровни защиты информации в компьютерных системах

Организация системы безопасности по уровням компьютерных систем (КС). Уровни защиты, в соответствии с механизмами реагирования на угрозы. Способы защиты данных на различных уровнях. Организация системы безопасности по уровням.

Машинные носители информации (МНИ). Защита МНИ. Защита средств взаимодействия с МНИ.

Основные особенности компьютерной информации с точки зрения доступа к ней злоумышленников. Виды защищаемой компьютерной информа-

ции. Условия доступа к защищаемой информации со стороны злоумышленников.

Тема 4. Основные положения формальной теории защиты информации

Аксиомы и определения доступа субъектов к объектам. Понятие объекта относительно языка L. Объекты, входящие в состав КС. Язык описания клавиатуры. Преобразование. Пример преобразования. Инициирование действия преобразования. Два состояния преобразования. Понятие домена. Процесс. Определение субъекта. Виды доступа к субъекту. Информационный поток. Запись.

Аксиома доступа субъектов к объектам. Определение понятия разграничения доступа. Методы разграничения доступа.

Дискреционное разграничение доступа. Матрицы доступа. Списки полномочий.

Полномочное (мандатное) разграничение доступа. Разграничение по уровням секретности. Различие между дискреционным и мандатным разграничением доступа.

Тема № 5. Формальные модели безопасности

Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU). Моделирование поведения системы во времени. Основные команды и операции, моделирующие поведение системы. Примеры команд, используемых при переходе системы из одного состояния в другое. Формальное описание системы в модели HRU. Поведение системы во времени. Понятие монооперационной системы. Теорема о существовании алгоритма определения исходного состояния системы. Условие использования классической модели HRU. Разрешимость проблемы безопасности.

Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

Граф доступов. Правила определения переходов системы из состояния в состояние. Условия реализации прав доступа. Расширенная модель Take-Grant, анализ информационных каналов.

Пути и стоимости возникновения информационных потоков в расширенной модели Take-Grant.

Тема № 6. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Тема № 7. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации

Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода. Организация защищенной среды обработки информации при комплексном подходе. Недостатки комплексного подхода. Условия эффективной работы средств защиты информации. Организация защиты субъектов информационных отношений.

Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

Построение систем защиты от угрозы нарушения конфиденциальности информации. Модель системы защиты от угроз нарушения конфиденциальности информации. Структура системы защиты от угроз нарушения конфиденциальности информации.

Построение систем защиты от угрозы нарушения целостности информации. Две основные группы организационно-технологических мер защиты целостности информации. Технологические меры контроля целостности битовых последовательностей, хранящихся на машинных носителях. Циклический контрольный код как механизм обеспечения контроля целостности информации. Интегрированный подход для обеспечения целостности данных. Основные принципы обеспечения целостности данных. Обеспечение защиты целостности программно-аппаратной среды.

Построение системы защиты от угрозы нарушения доступности информации. Понятие доступности информации. Основные угрозы доступности информации. Причины возникновения угроз доступности информации. Основные средства защиты от угрозы нарушения доступности информации.

Раздел 2. Прикладные основы теории компьютерной безопасности

Тема № 8. Методология обследования и проектирования защищенных информационных (автоматизированных) систем

Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Два основных метода проектирования. Метод проектирования «снизу вверх». Недостатки метода проектирования «снизу вверх». Иерархический метод построения защищённой АС («сверху вниз»). Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.

Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта. Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления

разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).

Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trusted computing base-TCB). Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2000). Цель создания АСЗИ.

Тема № 9. Общие сведения о стандартах в области информационной безопасности

Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ. Стандарты как основной механизм обеспечения совместимости продуктов и систем. Основы взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий (ИТ). Регламентация необходимости применения средств, механизмов, алгоритмов. Требования безопасности.

Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.

Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.

Набор требований к подсистемам защиты АС. Проверка соответствия требованиям по защите информации от НСД для АС. Показатели защищённости от НСД к информации в АС.

Стандарт «Критерии оценки доверенных компьютерных систем»/ TCSEC («Оранжевая книга»). Цель разработки стандарта TCSEC. Требования безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем. Категории требований безопасности. Общая структура требований к системам защиты.

Политика безопасности. Возможность осуществления субъектами доступа к объектам. Разграничение доступа к категорированной информации. Метки безопасности как механизм контроля доступа.

Аудит. Идентификация и аутентификация. Механизм защиты данных. Регистрация и учёт. Корректность. Контроль корректности функционирования средств защиты. Непрерывность защиты.

Основные положения «Общих критериев». Свойство «Общих критериев». Структура «Общих критериев». Определение объекта оценки и продукта. Система как специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Категории пользователей. Среда безопасности. Задачи, решаемые при подготовке к оценке. Требования по безопасности. Каталоги требований безопасности. Общая модель безопасности. Недостатки «Общих критериев».

Профили защиты. Введение профиля защиты. Идентификация профиля защиты. Аннотация профиля защиты. Описание объекта оценки. Характерные особенности ИТ применительно к объекту оценки (ОО).

Среда безопасности ОО. Описание аспектов безопасности среды, в которой предполагается использовать ОО. Структура и содержание профиля защиты. Цели безопасности для ОО. Цели безопасности для среды ОО.

Функциональные требования и требования доверия. Основные осуществляемые операции при выборе компонентов функциональных требований. Требования доверия к безопасности ОО. Обоснование профиля защиты.

Тема № 10. Концепция защиты СВТ и АС от НСД в соответствии с руководящими документами Гостехкомиссии и нормативно-методическими документами ФСТЭК России

Перечень основных документов ФСТЭК РФ по вопросам защиты информации. Основные положения концепции защиты СВТ и АС от НСД к информации. Определение НСД к информации. Два направления защиты от НСД. Особенности функций защиты в СВТ и АС. Основные способы НСД. Принципы защиты от НСД. Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ. Характеристики оценки технических средств защиты от НСД. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД. Проверка выполнения технических требований по защите. Сертификат соответствия СВТ или АС требованиям по защите.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине.

«Методические указания для обучающихся по освоению дисциплины»

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Теоретические основы компьютерной безопасности» приведена в Приложении 1 к настоящей рабочей программе.

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

Основная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597
2. Малюк А. А., Горбатов В. С. и др**.** Введение в информационную безопасность: Учебное пособие / Малюк А. А.,Горбатов В.С. и др. ; под. ред. В.С. Горбатого. - М.: Телеком, 2011. - 288 с.: ил. - ISBN 978-5-9912-0160-5.
3. Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

1. Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин Владимир Федорович. - Москва; Москва: Издательский Дом "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2014. - 416 с. - ДЛЯ УЧАЩИХСЯ ПТУ И СТУДЕНТОВ СРЕДНИХ СПЕЦИАЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-8199-0331-5. URL: http://znanium.com/go.php?id=423927
3. Цирлов В. Л. Основы информационной безопасности [Текст]: краткий курс / В. Л. Цирлов. - Ростов н/Д.: Феникс, 2008. - 253 с. - (Профессиональное образование). - ISBN 978-5-222-13164-0.

Рекомендуемая литература:

1. Ворона В. А., Тихонов В. А. Инженерно-техническая и пожарная защита объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2012. - 512 с.: ил. - ISBN 978-5-9912-0179-7.
2. Ворона В. А., Тихонов В. А. Технические средства наблюдения в охране объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2011. - 184 с.: ил. - ISBN 978-5-9912-0143-8.
3. Зайцев А. П. и др**.** Технические средства и методы защиты информации [Текст]: учебное пособие для вуза / Зайцев А.П. и др.; под. ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - М.: Горячая линия-Телеком, 2012. - 616 с.: ил. - ISBN 978-5-9912-0084-4.
4. Ярочкин В. И. Информационная безопасность / В. И. Ярочкин; В.И. Ярочкин. - 5-е изд. - Москва: Академический проект, 2008. - 544 с. - (Gaudeamus). - ISBN 978-5-8291-0987-5. URL: http://biblioclub.ru/index.php?page=book&id=211164.

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

Интернет-ресурсы:

http://www.gov.ru - сервер органов государственной власти Российской Федерации.

http://www.minfin.ru - официальный сайт Министерства финансов Российской Федерации.
http://www.znanium.com/ - электронно-библиотечная система
http://www.e.lanbook.com/ - ЭБС Издательства "ЛАНЬ"
http://www.rucont.ru/- электронно-библиотечная система
http://www.biblioclub.ru/ -университетская библиотека онлайн

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

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

Перечень программного обеспечения: *MS Office*
Информационные справочные системы: *Электронные ресурсы образовательной среды Университета.*

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

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7; программы эмуляции виртуальных машин (VM-vare, VM-box или др.); операционная система MS Windows Server 2003 или др. сетевая ОС.
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 09.04.03 Прикладная информатика

Профиль: Моделирование и проектирование информационных систем

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1.Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся приобретает:		
				Необходимые знания	Необходимые умения	Трудовые действия
1.	ПК-1	Способность применять современные методы и инструментальные средства прикладной информатики для автоматизации решения прикладных задач различных классов и создания ИС	Тема:1-5	Имеет понятие о методах и инструментальных средствах прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	Использует методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	Применяет методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС
2.	ПК-5	Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	Тема:1-5	Понимает передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	Использует передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	Применяет передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	**Инструменты, оценивающие сформированность компетенции**	**Этапы и показатель оценивания компетенции**	**Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания**
ПК-1 ПК-5	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-1 ПК-5	Выполнение контрольной работы	А) **полностью сформирована** (компетенция освоена на высоком уровне) – 5 баллов Б) **частично сформирована**: •компетенция **освоена на продвинутом уровне** – 4 балла; •**компетенция освоена на базовом уровне** – 3 балла; В) **не сформирована** (компетенция не освоена) – 2 и менее баллов	При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1 Примерная тематика докладов в форме презентаций:

1. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Основы обеспечения безопасности информации в компьютерных системах.
2. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.
3. Проектирование архитектуры системы защиты информации выбранного объекта и оценка его уровня защищённости.
4. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
5. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.
6. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию.
7. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.
8. Разработка проекта создания системы защиты информации на выбранных типовых офисных объектах.
9. Основные виды атак на компьютерные системы (КС), их классификация, проблемы обеспечения информационной безопасности в проводных КС.
10. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.
11. Компьютерная преступность в экономических областях.
12. Компьютерные вирусы в современных информационных системах.
13. Информационные угрозы современным экономическим объектам.
14. Безопасность информации в коммерческой деятельности.
15. Становление и развитие промышленного шпионажа.

16. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.
17. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).
18. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.
19. Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).
20. Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине является экзамен, проводимый в письменной форме по материалам лекций и выполненных практических заданий

Неделя текущего контроля	**Вид оценочного средства**	**Код компетенций, оценивающий знания, умения, навыки**	**Содержание оценочного средства**	**Требования к выполнению**	**Срок сдачи (неделя семестра)**	**Критерии оценки по содержанию и качеству с указанием баллов**
Проводится в сроки, установленные графиком образовательного процесса	Экзамен	ПК-1 ПК-5	2 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 20 минут на каждого студента	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на прак-

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
						тических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «**Удовлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

4.2. Типовые вопросы, выносимые на экзамен

1. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности.
2. Структура информационных ресурсов и администрирование в компьютерных системах.
3. Проблемы безопасности компьютерных систем (сетей), понятие угрозы, цели злоумышленников, осуществляющих основные атаки.

4. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников

5. Уязвимости автоматизированных систем (АС), возможные атаки на них. Особенности построения систем обнаружения атак (СОА) в АС.

6. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.

7. Факторы, воздействующие на защищаемую информацию. Классификация угроз. Естественные и искусственные угрозы. Основные направления и методы реализации угроз.

8. Основные виды атак на КС, их классификация. Проблемы обеспечения информационной безопасности в проводных КС.

9. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

10. Основные уровни защиты информации в компьютерных системах, организация системы безопасности по уровням компьютерных систем, уровни защиты, в соответствии с механизмами реагирования на угрозы.

11. Машинные носители информации (МНИ), защита МНИ, защита средств взаимодействия с МНИ.

12. Методы и средства обеспечения защиты информации в компьютерных системах, защита представления информации, защита содержания информации.

13. Представьте обобщенную модель защиты объекта, содержащего локальную вычислительную сеть, с безопасной обработкой информации.

14. Какие стадии включает жизненный цикл системы защиты информации (СЗИ), если СЗИ рассматривать как сложную техническую систему? Охарактеризуйте какие процессы включает каждая из стадий.

15. Какие объекты информатизации, инженерные, технические и программно-аппаратные способы и средства могут быть использованы для защиты информации в коммерческих структурах?

16. Перечислите рекомендуемые СТР-К стадии создания системы защиты информации (СЗИ). Какие вопросы решаются на предпроектной стадии, кем она выполняется и чем заканчивается.

17. Сертификация программных и программно-технических средств защиты конфиденциальной компьютерной информации.

18. Методы обеспечения защиты информации – препятствие, маскировка, управление доступом. Функции защиты при управлении доступом. Принуждение и побуждение.

19. Физические средства защиты компьютерных систем. Нейтрализация утечки информации по электромагнитным каналам – применение генераторов шума. Защита от наводок.
20. Аксиомы и определения доступа субъектов к объектам. Понятие объекта относительно языка L. Объекты, входящие в состав компьютерных систем.
21. Аксиома доступа субъектов к объектам. Определение понятия разграничения доступа. Методы разграничения доступа.
22. Дискреционное разграничение доступа. Матрицы доступа. Списки полномочий.
23. Полномочное (мандатное) разграничение доступа. Разграничение по уровням секретности. Различие между дискреционным и мандатным разграничением доступа.
24. Концепция монитора безопасности обращений в компьютерную систему. Правила разграничения доступа субъектов к объектам в ОС.
25. Монитор безопасности обращений (МБО) субъектов к объектам. Схема монитора безопасности обращений. Функции МБО. Свойства МБО.
26. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана.
27. Формальное описание системы в модели Харрисона-Руззо-Ульмана. Поведение системы во времени. Понятие монооперационной системы.
28. Теорема о существовании алгоритма определения исходного состояния системы. Условие использования классической модели Харрисона-Руззо-Ульмана. Разрешимость проблемы безопасности.
29. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.
30. Граф доступов. Правила определения переходов системы из состояния в состояние. Условия реализации прав доступа. Расширенная модель Take-Grant, анализ информационных каналов.
31. Пути и стоимости возникновения информационных потоков в расширенной модели Take-Grant.
32. Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).
33. Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.

34. Условие определения безопасности системы. Свойства безопасности системы. Проверка безопасности системы. Основные теоремы и определения состояний системы.
35. Эквивалентные подходы к определению безопасности модели Белла-Лападулы. Недостатки модели Белла-Лападулы.
36. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.
37. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
38. Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.
39. Реализация политики безопасности в компьютерных системах (КС) с использованием механизмов и средств операционных систем. Управление доступом в КС с использованием механизмов и средств сетевых операционных систем.
40. Управление инцидентами информационной безопасности в компьютерных системах.
41. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.
42. Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода. Организация защищенной среды обработки информации при комплексном подходе. Недостатки комплексного подхода.
43. Построение систем защиты от угрозы нарушения конфиденциальности информации. Модель системы защиты от угроз нарушения конфиденциальности информации. Структура системы защиты от угроз нарушения конфиденциальности информации.
44. Построение систем защиты от угрозы нарушения целостности информации. Две основные группы организационно-технологических мер защиты целостности информации. Технологические меры контроля целостности битовых последовательностей, хранящихся на машинных носителях.
45. Построение системы защиты от угрозы нарушения доступности информации. Понятие доступности информации. Основные угрозы доступности информации. Причины возникновения угроз доступности информации. Основные средства защиты от угрозы нарушения доступности информации.
47. Особенности построения парольных систем аутентификации. Парольная защита. Понятия идентификатора и пароля пользователя. Учетная запись

пользователя как совокупность его идентификатора и его пароля. Парольная система и состав её элементов.

48. Основные угрозы безопасности парольных систем. Способы получения пароля злоумышленником. Рекомендации по практической реализации парольных систем. Оценка стойкости парольных систем. Методы хранения и передачи паролей. Механизмы хранения паролей в КС.

49. Проблема организации совместного доступа различных приложений к некоторым областям памяти. Основные способы защиты памяти. Барьерные адреса. Механизм функционирования барьерного способа защиты памяти. Способы задания барьерного адреса. Динамические области памяти. Защита данных приложений.

50. Адресные регистры. Особенности способов защиты памяти. Ключ доступа. Организация совместного использования областей памяти. Механизм страничной организации памяти и сегментации.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

Приложение 2

ИНСТИТУТ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 09.04.03 Прикладная информатика

Профиль: Моделирование и проектирование информационных систем

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Целью изучения дисциплины является:
1. Сформировать у студентов базовые знания и практические навыки защиты информации в компьютерных системах.
2. Освоение студентами теоретических основ, технологий и механизмов защиты компьютерных систем.

Основными **задачами** дисциплины являются:
1. ознакомление студентов с теоретическими основами и нормативной базой, применяемых для построения защищенных информационных систем;
2. формирование у студентов базовых знаний в области технологий и механизмов защиты информации, применяемых в компьютерных системах;
3. привитие студентам навыков практической работы с программно-аппаратными средствами защиты информации;
4. подготовка студентов применять стандарты по оценке информационной защищённости при анализе и проектировании защищённых компьютерных систем.

2. Указания по проведению практических занятий

Тема 2. Анализ угроз информационной безопасности для компьютерных систем

Практическое занятие 1

*Вид практического занятия***:** смешанная форма практического занятия.
Образовательные технологии: самостоятельное решение и групповое обсуждение результатов.
Тема и содержание практического занятия: Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. Уязвимости АС, возможные атаки на них. Особенности построения систем обнаружения атак (СОА) в АС. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).
Цель работы: Получить практические знания и навыки об угрозах и возможных атаках, которым могут быть подвергнуты информационные системы.

Учебные вопросы:

- Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
- Уязвимости АС, возможные атаки на них.
- Особенности построения систем обнаружения атак (СОА) в АС.
- Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.

• Причины возникновения угроз безопасности информации. Отличительные особенности угроз корпоративным и локально-вычислительным сетям.
Продолжительность занятия -2ч.

Тема 3. Основные уровни защиты информации в компьютерных системах

Практическое занятие 2

*Вид практического занятия***:** смешанная форма практического занятия.
Образовательные технологии: самостоятельное решение и групповое обсуждение результатов.
Тема и содержание практического занятия:
Цель работы: Получить практические знания и навыки об уровнях защиты информации в компьютерных системах.

Учебные вопросы:

• Организация системы безопасности по уровням компьютерных систем (КС). Уровни защиты, в соответствии с механизмами реагирования на угрозы.

• Способы защиты данных на различных уровнях. Организация системы безопасности по уровням.

• Машинные носители информации (МНИ). Защита МНИ. Защита средств взаимодействия с МНИ.

• Основные особенности компьютерной информации с точки зрения доступа к ней злоумышленников.

• Виды защищаемой компьютерной информации.

• Условия доступа к защищаемой информации со стороны злоумышленников.

Продолжительность занятия -2ч.

Тема 4. Основные положения формальной теории защиты информации

Практическое занятие 3

*Вид практического занятия***:** смешанная форма практического занятия.
Образовательные технологии: самостоятельное решение и групповое обсуждение результатов.
Тема и содержание практического занятия: Аксиомы и определения доступа субъектов к объектам. Понятие объекта относительно языка L. Объекты, входящие в состав КС. Язык описания клавиатуры. Преобразование. Пример преобразования. Инициирование действия преобразования. Два состояния преобразования. Понятие домена. Процесс. Определение субъекта. Виды доступа к субъекту. Информационный поток. Запись.
Цель работы: Получить практические знания и навыки по методам разграничения доступа в информационных системах.

Учебные вопросы:

• Аксиома доступа субъектов к объектам.

• Определение понятия разграничения доступа. Методы разграничения доступа.

• Дискреционное разграничение доступа. Матрицы доступа. Списки полномочий.

• Полномочное (мандатное) разграничение доступа. Разграничение по уровням секретности.

• Различие между дискреционным и мандатным разграничением доступа.

• Ролевое разграничение доступа.

Продолжительность занятия -2ч.

Тема 5. Формальные модели безопасности

Практическое занятие 4

*Вид практического занятия***:** смешанная форма практического занятия.

Образовательные технологии: самостоятельное решение и групповое обсуждение результатов.

Тема и содержание практического занятия: Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU). Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

Цель работы: получить практические знания и навыки об основных формальных логических моделях доступа.

Учебные вопросы:

• Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).

• Моделирование поведения системы во времени. Основные команды и операции, моделирующие поведение системы. Примеры команд, используемых при переходе системы из одного состояния в другое.

• Формальное описание системы в модели HRU. Поведение системы во времени.

• Понятие монооперационной системы. Теорема о существовании алгоритма определения исходного состояния системы. Условие использования классической модели HRU. Разрешимость проблемы безопасности.

• Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant.

• Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

• Граф доступов. Правила определения переходов системы из состояния в состояние. Условия реализации прав доступа.

• Расширенная модель Take-Grant, анализ информационных каналов.

• Пути и стоимости возникновения информационных потоков в расширенной модели Take-Grant.

Продолжительность занятия -2ч.

Тема 6. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Практическое занятие 5

Вид практического занятия: смешанная форма практического занятия.

Образовательные технологии: самостоятельное решение и групповое обсуждение результатов.

Тема и содержание практического занятия: Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.

Учебные вопросы:

- Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.
- Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
- Требования, предъявляемые к формированию политики безопасности организации.
- Структура и содержание политики безопасности организации применительно к компьютерным системам.
- Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.

Продолжительность занятия -2ч.

Тема 7. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации

Практическое занятие 6

Вид практического занятия: смешанная форма практического занятия.

Образовательные технологии: самостоятельное решение и групповое обсуждение результатов.

Тема и содержание практического занятия: Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода. Организация защищенной среды обработки информации при комплексном подходе. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

Цель работы: получить практические знания и навыки по построению систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

Учебные вопросы:

• Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода.

• Организация защищенной среды обработки информации при комплексном подходе. Недостатки комплексного подхода. Условия эффективной работы средств защиты информации.

• Организация защиты субъектов информационных отношений.

• Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

• Построение систем защиты от угрозы нарушения конфиденциальности информации. Модель системы защиты от угроз нарушения конфиденциальности информации. Структура системы защиты от угроз нарушения конфиденциальности информации.

• Построение систем защиты от угрозы нарушения целостности информации. Две основные группы организационно-технологических мер защиты целостности информации.

• Технологические меры контроля целостности битовых последовательностей, хранящихся на машинных носителях.

• Циклический контрольный код как механизм обеспечения контроля целостности информации.

• Интегрированный подход для обеспечения целостности данных. Основные принципы обеспечения целостности данных. Обеспечение защиты целостности программно-аппаратной среды.

• Построение системы защиты от угрозы нарушения доступности информации. Понятие доступности информации.

• Основные угрозы доступности информации. Причины возникновения угроз доступности информации.

• Основные средства защиты от угрозы нарушения доступности информации.

Продолжительность занятия -2ч.

Тема 8. Методология обследования и проектирования защищенных информационных (автоматизированных) систем

Практическое занятие 7

Вид практического занятия: смешанная форма практического занятия.

Образовательные технологии: самостоятельное решение и групповое обсуждение результатов.

Тема и содержание практического занятия: Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований. Теория безопасных систем (TCB). Понятие «доверенная вычислительная среда» (trusted computing base-TCB). Дискретная природа характеристики «безопасный». Характеристика «доверенный».

Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2000).

Цель работы: получить практические знания и навыки об этапах и содержании работ по проектированию защищенных информационных (автоматизированных) систем.

Учебные вопросы:

- Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи.
- Методы построения защищённых АС. Два основных метода проектирования. Метод проектирования «снизу вверх». Недостатки метода проектирования «снизу вверх».
- Иерархический метод построения защищённой АС («сверху вниз»).
- Принципы проектирования. Структурный принцип и принцип модульного проектирования.
- Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.
- Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта.
- Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).
- Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.
- Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trusted computing base-TCB).
- Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду.
- Этапы разработки защищённой автоматизированной системы (АСЗИ). Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.

Продолжительность занятия -2ч.

Тема 9. Общие сведения о стандартах в области информационной безопасности

Практическое занятие 9

Вид практического занятия: смешанная форма практического занятия.
Образовательные технологии: самостоятельное решение и групповое обсуждение результатов.
Тема и содержание практического занятия: Профили защиты. Введение профиля защиты. Идентификация профиля защиты. Аннотация профиля защиты. Описание объекта оценки. Характерные особенности ИТ применительно к объекту оценки (ОО). Функциональные требования и требования доверия. Основные осуществляемые операции при выборе компонентов функциональных требований. Требования доверия к безопасности ОО. Обоснование профиля защиты.
Цель работы: получить практические знания и навыки о применении стандартов в области информационной безопасности

Учебные вопросы:

- Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.
- Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.
- Стандарт «Критерии оценки доверенных компьютерных систем»/ TCSEC («Оранжевая книга»). Цель разработки стандарта TCSEC. Требования безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем. Категории требований безопасности. Общая структура требований к системам защиты.
- Политика безопасности. Возможность осуществления субъектами доступа к объектам. Разграничение доступа к категорированной информации. Метки безопасности как механизм контроля доступа.
- Основные положения «Общих критериев». Свойство «Общих критериев». Структура «Общих критериев». Определение объекта оценки и продукта. Система как специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.
- Среда безопасности ОО. Описание аспектов безопасности среды, в которой предполагается использовать ОО. Структура и содержание профиля защиты. Цели безопасности для ОО. Цели безопасности для среды ОО.
- Функциональные требования и требования доверия. Основные осуществляемые операции при выборе компонентов функциональных требований. Требования доверия к безопасности ОО. Обоснование профиля защиты.

Продолжительность занятия -2ч.

3. Указания по проведению лабораторных работ.

Не предусмотрены учебным планом.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Анализ угроз информационной безопасности для компьютерных систем	***Подготовка докладов и презентаций по темам:*** Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
2	Основные уровни защиты информации в компьютерных системах	***Подготовка докладов и презентаций по темам:*** Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
3	Основные положения формальной теории защиты информации	***Подготовка докладов и презентаций по темам:*** Перечень основных документов ФСТЭК России по вопросам защиты информации. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД.
4	Формальные модели безопасности	***Подготовка докладов и презентаций по темам:*** Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ. Базовая модель угроз ИСПДн. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.
5	Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам	***Подготовка докладов и презентаций по темам:*** Лицензирование и сертификация в области защиты информации. Комплексные системы защиты информации. Аттестация АС по требованиям безопасности информации.
6	Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации	***Подготовка докладов и презентаций по темам:*** Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU). Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Преимущества использования модульного принципа.

5. Указания по проведению контрольных работ для обучающихся очной формы обучения

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую Вами литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 10 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4 Тематика контрольной работы

1. Цифровая подпись. Проблема аутентификации данных или цифровой подписи. Модель аутентификации сообщений. Сравнительный анализ обычной и цифровой подписи.

2. Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС.

3. Что означает термин «аттестация объекта информатизации», раскройте это понятие, какие процедуры предусматриваются для аттестации автоматизированной системы?

4. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания автоматизированных систем в защищенном исполнении.
5. Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ.
6. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.
7. Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.

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

Основная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597
2. Малюк А. А., Горбатов В. С. и др. Введение в информационную безопасность: Учебное пособие / Малюк А. А.,Горбатов В.С. и др. ; под. ред. В.С. Горбатого. - М.: Телеком, 2011. - 288 с.: ил. - ISBN 978-5-9912-0160-5.
3. Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

1. Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин Владимир Федорович. - Москва; Москва: Издательский Дом "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2014. - 416 с. - ДЛЯ УЧАЩИХСЯ ПТУ И СТУДЕНТОВ СРЕДНИХ СПЕЦИАЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-8199-0331-5. URL: http://znanium.com/go.php?id=423927
3. Цирлов В. Л. Основы информационной безопасности [Текст]: краткий курс / В. Л. Цирлов. - Ростов н/Д.: Феникс, 2008. - 253 с. - (Профессиональное образование). - ISBN 978-5-222-13164-0.

Рекомендуемая литература:

1. Ворона В. А., Тихонов В. А. Инженерно-техническая и пожарная защита объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2012. - 512 с.: ил. - ISBN 978-5-9912-0179-7.
2. Ворона В. А., Тихонов В. А. Технические средства наблюдения в охране объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2011. - 184 с.: ил. - ISBN 978-5-9912-0143-8.
3. Зайцев А. П. и др. Технические средства и методы защиты информации [Текст]: учебное пособие для вуза / Зайцев А.П. и др.; под. ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - М.: Горячая линия-Телеком, 2012. - 616 с.: ил. - ISBN 978-5-9912-0084-4.
4. Ярочкин В. И. Информационная безопасность / В. И. Ярочкин; В.И. Ярочкин. - 5-е изд. - Москва: Академический проект, 2008. - 544 с. - (Gaudeamus). - ISBN 978-5-8291-0987-5. URL: http://biblioclub.ru/index.php?page=book&id=211164.

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

Интернет-ресурсы:

http://www.gov.ru - сервер органов государственной власти Российской Федерации.

http://www.minfin.ru - официальный сайт Министерства финансов Российской Федерации.

http://www.znanium.com/ - электронно-библиотечная система

http://www.e.lanbook.com/ - ЭБС Издательства "ЛАНЬ"

http://www.rucont.ru/- электронно-библиотечная система

http://www.biblioclub.ru/ -университетская библиотека онлайн

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

Перечень программного обеспечения: *MS Office*

Информационные справочные системы: *Электронные ресурсы образовательной среды Университета.*