

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Петренко Вячеслав Иванович
 Должность: и.о. директора Института цифрового развития
 Дата подписания: 05.07.2024 09:35:26
 Уникальный программный ключ:
 b47f96eea65a2d6e27b974ab71b0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Модели безопасности компьютерных систем
Содержание	Информационные модели. Общая математическая модель защиты информации. Вспомогательные структуры (модели), используемые в защите информации. Основы политики и моделей безопасности информации. Модели дискреционного доступа. Модели мандатного контроля и управления доступом. Основные понятия теории нечетких множеств. Общая характеристика проблемы синтеза систем защиты информации для информационных систем.
Реализуемые компетенции	ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.
Результаты освоения дисциплины (модуля)	ОПК-6 Знать: систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем. Уметь: разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы. ОПК-11 Знать: основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; средства и методы хранения и передачи

	аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем. Уметь: разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем. Владеть: способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах; средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем; навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.
Трудоемкость, з.е.	4
Формы отчетности	Зачет с оценкой, 8 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Девянин П.Н. Управление доступом и информационными потоками: учебное пособие для студентов высших учебных заведений, обучающихся по специальностям направления подготовки 090300 – "Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем" и направлению подготовки 090900 – "Информационная безопасность" / П. Н. Девянин. Москва, 2011. 2. Гульяев А. Визуальное моделирование в среде MATLAB. – СПб: Питер, – 2010. – 432 с. 3. Емельянов В.В., Майорова В.И., Разумцова Ю.В. и др. Принятие оптимальных решений в интеллектуальных имитационных системах: Учебное пособие по курсам «Методы системного анализа и синтеза» и «Моделирование технологических и производственных процессов» – М.: Изд-во МГТУ им. Н.Э. Баумана, – 2010.
Дополнительная литература	1. Вендров А.М. Проектирование программного обеспечения экономических информационных систем. Учеб. - М.: Финансы и статистика. – 2010. 2. Девянин П.Н. Модели безопасности компьютерных систем. Учеб. пособие для студентов вузов, обучающихся по специальности 075200 "Компьютер. безопасность" и 075500 "Комплекс. обеспечение информ. безопасности автоматизир. систем" - Москва, Сер. Высшее профессиональное образование. Информационная безопасность, 2005. 3. Емельянов А.А. и др. Имитационное моделирование экономических процессов: Учебное пособие / А.А. Емельянов, Е.А. Власова, Р.В. Дума; Под ред. А.А. Емельянова. – М.: Финансы и статистика, 2009. 4. Карпов Ю. Имитационное моделирование систем. Введение в

	моделирование с AnyLogic 5. - СПб.: БХВ-Петербург, 2005. 5. Модели безопасности компьютерных систем: учебно-метод. пособие: Специальность 090301.65 - Компьютерная безопасность. Специализация "Информационная безопасность объектов информатизации на базе компьютерных систем", "Разработка защищенного программного обеспечения", "Математические методы защиты информации". Специалитет / сост. И. В. Зайцева; Сев.-Кав. федер. ун-т. – Ставрополь: СКФУ, 2014. – 108 с.
--	--