

АННОТАЦИЯ ДИСЦИПЛИНЫ

«Информационная безопасность автоматизированных банковских систем»

Дисциплина «Информационная безопасность автоматизированных банковских систем» является частью программы специалитета «Безопасность открытых информационных систем (СУОС)» по направлению «10.05.03 Информационная безопасность автоматизированных систем».

Цели и задачи дисциплины

Цель дисциплины – освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе реализации требований к информационной безопасности автоматизированных банковских систем. Задачи дисциплины: - изучение основных положений, понятий и категорий теоретических основ функционирования систем информационной безопасности автоматизированных банковских систем; - изучение основ и принципов организации современных проблем организационного обеспечения информационной безопасности; - изучение организации работы и порядка применения терминологии организационного обеспечения информационной безопасности; - изучение целей систем организационной защиты информации автоматизированных банковских систем; - изучение основных направлений и методов организационной защиты информации автоматизированных банковских систем, формирование умений в разработке проектов функционирования систем организационной защиты информации автоматизированных банковских систем; - формирование навыков работы в организации процессов управления системами организационной защиты информации автоматизированных банковских систем..

Изучаемые объекты дисциплины

- методы правовой защиты информации в автоматизированных банковских системах; - правовые основы защиты персональных данных в автоматизированных банковских системах; - правовые основы деятельности подразделений защиты информации автоматизированных банковских систем; - порядок организации охраны объектов информатизации, внутриобъектового и пропускного режима автоматизированных банковских систем; - организация работы с персоналом по вопросам защиты информации в банковской сфере; - организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам в банковской сфере; - организация деятельности службы безопасности в банковской сфере..

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		10	11
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	126	72	54
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	60	36	24
- лабораторные работы (ЛР)	32	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	30	18	12
- контроль самостоятельной работы (КСР)	4	2	2
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	126	72	54
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет	9		9
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	288	180	108

Краткое содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
10-й семестр				
Обеспечение информационной безопасности и защита автоматизированных систем	12	8	10	30
Шифрование данных при хранении и передачи (симметричное/асимметричное шифрование). Понятие электронной подписи, цифровых сертификатов, описание механизмов аутентификации. Политика безопасности в системе, критичные информационные ресурсы. Разграничение доступа к ресурсам, понятие несанкционированного доступа и несанкционированного воздействия. Понятие целостности и лицензионной чистоты программного обеспечения.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Общие понятия об информационных технологиях	10	4	4	20
Аппаратное и программное обеспечение вычислительной техники, информационные процессы и информационные технологии. Системное и прикладное программное обеспечение, понятие информационных ресурсов (объектов) и пользователей данных ресурсов (субъектов). Основные функции операционной системы ПЭВМ, встроенные возможности разграничения доступа, блокировка доступа к рабочей станции. Идентификация и аутентификация пользователей автоматизированных систем, понятие учетных записей, полномочия администраторов и пользователей систем (привилегии, роли), автоматическая блокировка/разблокировка учетных записей. Использование паролей, понятие структуры пароля, правила выбора стойких паролей, подбор паролей с использование специализированных программ. Использование локально-вычислительных сетей, понятие сетевых ресурсов, изолированность сегментов локально-вычислительных сетей, разграничение прав доступа к сетевым ресурсам (на примере сети в Windows и Linux), анализ системных журналов, резервирование и архивирование данных.				
Информационная безопасность в системе Банка России. История банковского дела. Автоматизированные банковские системы.	12	4	4	22
Ростовщики. Трапезиты. История банков в России. Виды банков. Функции банков. Правовое регулирование банковской деятельностью. Особенности автоматизированных банковских систем, используемых в российских банках. Информационное обеспечение автоматизированных банковских систем. Техническое оснащение современных автоматизированных банковских систем. Программное обеспечение автоматизированных банковских систем.				
Введение	2	0	0	0
Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
курса и его место в подготовке специалистов по защите информации.				
ИТОГО по 10-му семестру	36	16	18	72
11-й семестр				
Информационная безопасности финансовой сферы. Пластиковые карты, электронные деньги. Реализация требований информационной безопасности в системе Банка России.	24	16	12	54
История развития Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (далее – ФинЦЕРТ). Цели и задачи ФинЦЕРТ. Основные направления деятельности центра. Автоматизация информационного обмена. Социальная инженерия. Борьба с СМС-рассылками и колл-центрами мошеннических структур. История развития пластиковых карт. История банковских карт в России. Виды электронных денег и их применение. Банкоматы. Банкоматное мошенничество. Криптовалюта. Основные направления политики информационной безопасности и нормативная база Банка России. Стандарты Банка России. Применяемые в ТУ Банка России меры и средства защиты информации, функции администраторов информационной безопасности подразделений. Особенности использования средств защиты информации от несанкционированного доступа. Организация бесперебойного функционирования информационных систем. Аудит информационной безопасности банковской системы. Тестирование на проникновение. Выявление известных уязвимостей ПО. Понятие инцидента, события и мошенничества в сфере банковской безопасности. Классификация нарушений безопасности в банковской сфере и примеры нарушений. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID. Профиль безопасности OpenID API для доступа к сервисам в режиме только для чтения. Профиль безопасности OpenID API для доступа к сервисам в режиме чтения и записи. Дистанционное банковское				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
обслуживание.				
ИТОГО по 11-му семестру	24	16	12	54
ИТОГО по дисциплине	60	32	30	126