МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
математического моделирования
_____ Костин В.А.
подпись
03.07.2018

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.34 Современные платежные системы и их безопасность
Код и наименование дисциплины в соответствии с Учебным планом

1. Шифр и наименование специальности:
10.05.04 Информационно-аналитические системы безопасности

2. Специализация:

Информационная безопасность финансовых и экономических структур

3. Квалификация (степень) выпускника: специалист

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины: математического моделирования математического факультета

6. Составитель программы: Костин Дмитрий Владимирович, к. ф.-м н,
ФИО, ученая степень, ученое звание

7. **Рекомендована:** научно-методическим советом математического факультета, протокол от 03.07.2018, № 0500-07
наименование рекомендующей структуры, дата, номер протокола

_____
отметки о продлении

8. Учебный год: 2018/2019 **Семестр(-ы): 7 , А**

9. Цели и задачи учебной дисциплины: Целью освоения дисциплины является подготовка обучающихся к научно-исследовательской деятельности по направлению подготовки 10.05.04 Информационно-аналитические системы безопасности посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части, представленных ниже знаний, умений и навыков. Задачами дисциплины является изучение понятийного аппарата дисциплины, основных теоретических положений и методов, привитие навыков применения теоретических знаний для решения практических задач.

10. Место учебной дисциплины в структуре ООП:

Учебная дисциплина «Радиоизмерения» относится к циклу «Дисциплины» Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.05.04 Информационно-аналитические системы безопасности (специалитет) и входит в базовую часть этого цикла.

Теоретической и практической основой для освоения учебной дисциплины «Современные платежные системы и их безопасность» являются знания, умения и навыки студентов, приобретенные ими в процессе освоения курсов «Информатика», «Организация ЭВМ и вычислительных систем», «Технология и методы программирования»

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-3	способностью применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности	***знать:*** Необходимо знать, как применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности ***уметь:*** применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности ***владеть:*** Необходимо владеть, способностью применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности
ОПК-7	способность применять методы и средства обеспечения информационной безопасности специальных ИАС	***знать:*** как применять методы и средства обеспечения информационной безопасности специальных ИАС ***уметь:*** применять методы и средства обеспечения информационной безопасности специальных ИАС ***владеть:*** способностью применять методы и средства обеспечения информационной безопасности специальных ИАС

ПСК-2.4	способность разрабатывать и применять автоматизированные технологии обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени	***знать:*** как разрабатывать и применять автоматизированные технологии обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени ***уметь:*** разрабатывать и применять автоматизированные технологии обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени ***владеть:*** способностью разрабатывать и применять автоматизированные технологии обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени

12 Объем дисциплины в зачетных единицах/часах (в соответствии с учебным планом) **— 4_ /_144**

Форма промежуточной аттестации (зачет/экзамен) – **экзамен**.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)		
	Всего	По семестрам	
		9 сем.	А сем.
Аудиторные занятия	60	36	24
в том числе: лекции	30	18	12
практические	0	0	0
лабораторные	30	18	12
Самостоятельная работа	48	36	12
Форма промежуточной аттестации *зачет – 0 час. / экзамен – __час.)*	**Экзамен 36**		**Экзамен 36**
Итого:	**144**	**72**	**72**

13.1. Содержание дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в проблему информационной безопасности . Основные положения функционирования системы расчетов и платежей.	1.Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. 2. Международные стандарты информационного обмена. Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации.

		3.Изучение договоров между банком и клиентом при проведении безналичных расчетов: договор расчетного счета; договор срочного вклада физического лица; договор банковского счета и кассового обслуживания
2	Правовые и организационные аспекты защиты информации.	1.Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно- справочные документы. 2..Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Компьютерные преступления. Организационное обеспечение информационной безопасности
3	Угрозы информационной безопасности и методы их реализации.	1.Три вида возможных нарушений информационной системы. 2.Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. 3.Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности ин- формации. 4. Информационная безопасность в условиях функционирования в России глобальных сетей
4	Методы и средства обеспечения информационной безопасности информационных систем	1.Общая проблема информационной безопасности информационных систем. 2. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение). 3. Основные технологии построения защищенных экономических информационных систем (ЭИС). 4.Защита информации от несанкционированного доступа. 5.Математические и методические средства защиты. Компьютерные средства реализации защиты в информационных системах.
5	Использование защищенных компьютерных систем	1.Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем. 2.Использование защищенных 5 компьютерных систем. Стандарты по оценке защищенных систем. Примеры практической реализации.
6	Защита от разрушающих программных воздействий.	1.Понятие разрушающего программного воздействия. Методы перехвата и навязывания информации. 2. Компьютерные вирусы. Понятия о видах вирусов.

		3. Современные антивирусные программы
7	Парольные системы. Электронные деньги и платежные карты	1.Общие подходы к построению парольных систем. 2.Выбор паролей. Хранение паролей. Передача пароля по сети. 3.Изучение расчетов пластиковыми картами.
8	Шифрование данных.	1.Особенности криптографического и стенографического преобразования информации. 2.Стойкость алгоритмов шифрования. Типы алгоритмов шифрования. 3. Примеры криптографических алгоритмов. 4.Особенности применения криптографических методов. 5.Особенности реализации систем с симметричными и несимметричными ключами. 6.Электронная подпись
9	Защита программ и данных	1.Базовые методы нейтрализации систем защиты от несанкционированного копирования. 2.Идентификация параметров персонального компьютера. 3.Идентификация жестких дисков. Идентификация гибких дисков. 4.Оценка уникальности конфигурации компьютера.
10	Особенности защиты в операционных системах.	1.Подходы к построению защищенной операционной системы. Административные меры защиты. 2. Стандарты защищенности операционных систем. Виды уязвимости и атак на ОС. 3. Классификация угроз безопасности операционной системы. Типичные атаки на операционную систему.
11	Особенности защиты информации в компьютерных сетях.	1.Классификация способов несанкционированного доступа и жизненный цикл атак. 2.Нападения на политику безопасности и процедуры административного управления. 3.Нападения на постоянные и сменные компоненты системы защиты. 4.Нападения на протоколы информационного взаимодействия. 5.Нападения на функциональные элементы компьютерных сетей. 6. Способы противодействия несанкционированному сетевому и межсетевому доступу. Аутентификация пользователя локальной сети. Разграничение доступа к локальной сети. 7.Противодействие несанкционированному межсетевому доступу. 8.Использование межсетевых экранов (Firewall). Критерии их оценки.
12	Особенности защиты информации в СУБД	1.Защита базы данных и ее элементов. Привилегии пользователей.

		2.Защита баз данных в MS ACCESS. Выбор модели безопасности MS SQL Server. 3.Соотнесение бюджетов пользователей Windows 2000 и идентификаторов SQL Server. Владельцы объектов SQL Server и права доступа к объекту. 4.Доступ к SQL Server по коммутируемым каналам. Резервное сохранение и восстановление данных в SQL Server.
13	Схемы проведения платежей (валовые и нетто расчеты). Ключевые принципы для системно значимых платежных систем	1.Изучение схем проведения платежей, валовые расчеты. 2. Изучение ключевых принципов: правовая база проведения расчетов, управление рисками, обеспечение ликвидности, критерии участия.

13.2 Темы (разделы) дисциплины и виды занятий:

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные занятия	Самостоятельная работа	Всего
1	Введение в проблему информационной безопасности . Основные положения функционирования системы расчетов и платежей.	2	2	4	8
2	Правовые и организационные аспекты защиты информации.	2	2	4	8
3	Угрозы информационной безопасности и методы их реализации.	2	2	4	8
4	Методы и средства обеспечения информационной безопасности информационных систем	3	3	3	9
5	Использование защищенных компьютерных систем	3	3	3	9
6	Защита от разрушающих программных воздействий.	3	3	3	9
7	Парольные системы. Электронные деньги и платежные карты	2	2	4	8
8	Шифрование данных.	3	3	3	9
9	Защита программ и данных	2	2	4	8
10	Особенности защиты в операционных системах.	2	2	4	8
11	Особенности защиты информации в компьютерных сетях.	2	2	4	8
12	Особенности защиты информации в СУБД).	2	2	4	8

13	Схемы проведения платежей (валовые и нетто расчеты). Ключевые принципы для системно значимых платежных систем	2	2	4	8
	Итого:	**30**	**30**	**48**	**108**

14. Методические указания для обучающихся по освоению дисциплины
(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

При прохождении дисциплины используются активные и интерактивные формы проведения лекций и практических занятий и осуществляется контроль посещаемости и выполнения всех видов самостоятельной работы. В течение семестра студенты решают задачи, указанные преподавателем, к каждому занятию. В семестре проводится 2 контрольные работы (на лабораторных занятиях). Кроме того, предусмотрена работа с текстом конспекта лекции, изучение рекомендованной литературы, систематическая подготовка к лабораторным (семинарским) занятиям, выполнение домашних заданий.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список оформляется в соответствии с требованиями ГОСТ, используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	Макарова Наталья Владимировна. Информатика / Н.В. Макарова, В.Б. Волков — Санкт-Петербург [и др.] : Питер, 2015 .— 573 с.
2	Гринберг Анатолий Соломонович. Информационные технологии управления : учебное пособие для студ. вузов / А.С. Гринберг, Н.Н. Горбачев, А.С. Бондаренко .— М. : ЮНИТИ, 2004 .— 479 с. : ил., табл. — Библиогр.: с. 433-434

б) дополнительная литература:

№ п/п	Источник
3	Атака на Internet /Медведовский И.Д.,СемьяновП.В.,Леонов Д.Г.-2-е изд.,перераб. и доп.-М.:ДМК,1999
4	АнаньевАлександр. Самоучитель VisualBasic 6.0 / Александр Ананьев, Аркадий Федоров .— СПб. и др. : БХВ-Петербург, 2002 .— 622 с
5	ДомаревВ.В. Безопасность информационных технологий. Системный подход / В.В. Домарев .— М. ; СПб ; Киев : DiaSoft, 2004 .— 975 с.
6	Гринберг А.С. Защита информационных ресурсов государственного управления / А.С. Гринберг, Н.Н. Горбачев, А.А. Тепляков .— М. : ЮНИТИ, 2003 .— 327 с.

в)информационные электронно-образовательные ресурсы**:**

№ п/п	Источник

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы.

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

а) основная литература:	
б) дополнительная литература:	
в) информационные электронно-образовательные ресурсы:	

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости).

Стандартное современное программное обеспечение персонального компьютера, позволяющее, в том числе, писать и компилировать программы, эффективно использовать поисковые ресурсы глобальных сетей.

18. Материально-техническое обеспечение дисциплины:

1. Типовое оборудование компьютерного класса.
2. Программное обеспечение учебного процесса.

19. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения:

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОПК-1 способность анализировать физические явления и процессы, а также применять соответствующий математический аппарат при решении задач в сфере профессиональной деятельности	***знать:*** как анализировать физические явления и процессы, а также применять соответствующий математический аппарат при решении задач в сфере профессиональной деятельности		
	уметь: анализировать физические явления и процессы, а также применять соответствующий		

	математический аппарат при решении задач в сфере профессиональной деятельности		
	владеть: навыками и способностью анализировать физические явления и процессы, а также применять соответствующий математический аппарат при решении задач в сфере профессиональной деятельности		
ПК-15 способность применять современные методы научных исследований с использованием компьютерных технологий, в том числе в работе над междисциплинарными проектами	***знать:*** как применять современные методы научных исследований с использованием компьютерных технологий, в том числе в работе над междисциплинарными проектами		
	уметь: применять современные методы научных исследований с использованием компьютерных технологий, в том числе в работе над междисциплинарными проектами		
	Владеть: способностью применять современные методы научных исследований с использованием компьютерных технологий, в том числе в работе над междисциплинарными проектами		
ПК-16 способностью разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование	***знать:*** как разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и		

специальных ИАС и средств обеспечения их информационной безопасности	средств обеспечения их информационной безопасности ***уметь*** разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности ***Владеть:*** способностью разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности		
			КИМ № 1

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на зачете используются следующие ***показатели:***

1) знание основных возможностей решения интегральных уравнений

2) умение работать с прикладными программами и информационными ресурсами;

3) успешное прохождение текущей аттестации.

Для оценивания результатов обучения на зачете используется ***шкала:*** «зачтено», «незачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Полное соответствие ответа обучающегося всем перечисленным показателям по каждому из вопросов контрольно-измерительного материала.	Повышенный уровень	отлично

Несоответствие ответа обучающегося одному из перечисленных показателей (к одному из вопросов контрольно-измерительного материала) и правильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым двум из перечисленных показателей (либо двум к одному вопросу, либо по одному к каждому вопросу контрольно-измерительного материала) и правильные ответы на два дополнительных вопроса в пределах программы.	Базовый уровень	хорошо
Несоответствие ответа обучающегося любым двум из перечисленных показателей и неправильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым трем из перечисленных показателей (в различных комбинациях по отношению к вопросам контрольно-измерительного материала).	Пороговый уровень	удовлетворительно
Несоответствие ответа обучающегося любым четырем из перечисленных показателей (в различных комбинациях по отношению к вопросам контрольно-измерительного материала).	–	неудовлетворительно

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

19.3.1 Перечень вопросов к промежуточной аттестации – экзамену:

1. Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах.
2. Международные стандарты информационного обмена. Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации.
3. Изучение договоров между банком и клиентом при проведении безналичных расчетов: договор расчетного счета; договор срочного вклада физического лица; договор банковского счета и кассового обслуживания
4. Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно- справочные документы.
5.. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Компьютерные преступления. Организационное обеспечение информационной безопасности
6. Три вида возможных нарушений информационной системы.
7. Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации.
8. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации.
9. Информационная безопасность в условиях функционирования в России глобальных сетей
10. Общая проблема информационной безопасности информационных систем.

11. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение).
12. Основные технологии построения защищенных экономических информационных систем (ЭИС).
13. Защита информации от несанкционированного доступа.
14. Математические и методические средства защиты. Компьютерные средства реализации защиты в информационных системах.
15. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.
16. Использование защищенных компьютерных систем. Стандарты по оценке защищенных систем. Примеры практической реализации.
17. Понятие разрушающего программного воздействия. Методы перехвата и навязывания информации.
18. Компьютерные вирусы. Понятия о видах вирусов.
19. Современные антивирусные программы
20. Общие подходы к построению парольных систем.
21. Выбор паролей. Хранение паролей. Передача пароля по сети.
22. Изучение расчетов пластиковыми картами.
23. Особенности криптографического и стенографического преобразования информации. Стойкость алгоритмов шифрования. Типы алгоритмов шифрования.
24. Примеры криптографических алгоритмов. Особенности применения криптографических методов.
25. Особенности реализации систем с симметричными и несимметричными ключами.
26. Электронная подпись
27. Базовые методы нейтрализации систем защиты от несанкционированного копирования. Идентификация параметров персонального компьютера.
28. Идентификация жестких дисков. Идентификация гибких дисков. Оценка уникальности конфигурации компьютера.
29. Подходы к построению защищенной операционной системы. Административные меры защиты.
30. Стандарты защищенности операционных систем. Виды уязвимости и атак на ОС.
31. Классификация угроз безопасности операционной системы. Типичные атаки на операционную систему.
32. Классификация способов несанкционированного доступа и жизненный цикл атак.
33. Нападения на политику безопасности и процедуры административного управления.
34. Нападения на постоянные и сменные компоненты системы защиты.
35. Нападения на протоколы информационного взаимодействия.
36. Нападения на функциональные элементы компьютерных сетей.
37. Способы противодействия несанкционированному сетевому и межсетевому доступу. Аутентификация пользователя локальной сети. Разграничение доступа к локальной сети.
38. Противодействие несанкционированному межсетевому доступу.
39. Использование межсетевых экранов (Firewall). Критерии их оценки.
40. Защита базы данных и ее элементов. Привилегии пользователей.
41 Защита баз данных в MS ACCESS. Выбор модели безопасности MS SQL Server.
42. Соотнесение бюджетов пользователей Windows 2000 и идентификаторов SQL

Server. Владельцы объектов SQL Server и права доступа к объекту. .Доступ к SQL Server по коммутируемым каналам. Резервное сохранение и восстановление данных в SQL Server.

43. Изучение схем проведения платежей, валовые расчеты.
44. Изучение ключевых принципов: правовая база проведения расчетов, управление рисками, обеспечение ликвидности, критерии участия.

19.3.2 Перечень практических заданий для текущей аттестации: не предусмотрен

Критерии оценки компетенций (результатов обучения) при текущей аттестации (выполнении практических заданий):

– оценка «зачтено» ставится, если обучающийся продемонстрировал знание необходимого для выполнения лабораторной работы теоретического материала, показал владение практическими навыками и умение решать конкретную задачу в соответствии с поставленной целью. При этом допускается возможность, что были допущены незначительные неточности теоретического или практического плана;

– оценка «не зачтено» ставится, если обучающийся допустил существенную ошибку, связанную с незнанием теории или отсутствием необходимых умений и навыков для выполнения конкретной лабораторной работы.

19.3.3 Перечень тем рефератов для текущей аттестации: не предусмотрены.

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

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в форме устного опроса (индивидуального опроса, фронтальных бесед по вопросам семинарских занятий); оценки результатов практической деятельности (лабораторной работы). Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и умений.

При оценивании используются количественные шкалы оценок. Критерии оценивания приведены выше.

Форма контрольно-измерительного материала

УТВЕРЖДАЮ
Зав. кафедрой математического моделирования

_____ В.А. Костин
__.__.20__

Направление подготовки: 10.05.04 Информационно-аналитические системы безопасности
Дисциплина: Б1.В..34 Современные платежные системы и их безопасность
Курс: 5
Форма обучения: очная
Вид аттестации: промежуточная
Вид контроля: экзамен

Контрольно-измерительный материал № 14

1. Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах.
2. Международные стандарты информационного обмена. Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации.
3. Изучение договоров между банком и клиентом при проведении безналичных расчетов: договор расчетного счета; договор срочного вклада физического лица; договор банковского счета и кассового обслуживания
4. Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно- справочные документы.
5.. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Компьютерные преступления. Организационное обеспечение информационной безопасности
6. Три вида возможных нарушений информационной системы.
7. Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации.
8. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации.
9. Информационная безопасность в условиях функционирования в России глобальных сетей
15. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.
16. Использование защищенных 5 компьютерных систем. Стандарты по оценке защищенных систем. Примеры практической реализации.
17. Понятие разрушающего программного воздействия. Методы перехвата и навязывания информации.
18. Компьютерные вирусы. Понятия о видах вирусов.
19. Современные антивирусные программы
20. Общие подходы к построению парольных систем.
21. Выбор паролей. Хранение паролей. Передача пароля по сети.
22. Изучение расчетов пластиковыми картами.

23. Особенности криптографического и стенографического преобразования информации. Стойкость алгоритмов шифрования. Типы алгоритмов шифрования.
24. Примеры криптографических алгоритмов. Особенности применения криптографических методов.
25. Особенности реализации систем с симметричными и несимметричными ключами.
26. Электронная подпись
27. Базовые методы нейтрализации систем защиты от несанкционированного копирования..Идентификация параметров персонального компьютера.
28. Идентификация жестких дисков. Идентификация гибких дисков..Оценка уникальности конфигурации компьютера.
29. Подходы к построению защищенной операционной системы. Административные меры защиты.
30. Стандарты защищенности операционных систем. Виды уязвимости и атак на ОС.
31. Классификация угроз безопасности операционной системы. Типичные атаки на операционную систему.
32. Классификация способов несанкционированного доступа и жизненный цикл атак.
33. Нападения на политику безопасности и процедуры административного управления.
34. Нападения на постоянные и сменные компоненты системы защиты.
35. Нападения на протоколы информационного взаимодействия.
36. Нападения на функциональные элементы компьютерных сетей.
37. Способы противодействия несанкционированному сетевому и межсетевому доступу. Аутентификация пользователя локальной сети. Разграничение доступа к локальной сети.
38. Противодействие несанкционированному межсетевому доступу.
39. Использование межсетевых экранов (Firewall). Критерии их оценки.
40. Защита базы данных и ее элементов. Привилегии пользователей.
41 Защита баз данных в MS ACCESS. Выбор модели безопасности MS SQL Server.
42. Соотнесение бюджетов пользователей Windows 2000 и идентификаторов SQL Server. Владельцы объектов SQL Server и права доступа к объекту..Доступ к SQL Server по коммутируемым каналам. Резервное сохранение и восстановление данных в SQL Server.
43. Изучение схем проведения платежей, валовые расчеты.
44. Изучение ключевых принципов: правовая база проведения расчетов, управление рисками, обеспечение ликвидности, критерии участия.

Преподаватель _____ Костин А.В

ЛИСТ СОГЛАСОВАНИЙ

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальность 10.05.04 *Информационно-аналитические системы безопасности*
шифр и наименование направления/специальности

Дисциплина *Б1.В.34 Современные платежные системы и их безопасность*
код и наименование дисциплины

Специализация *Информационная безопасность финансовых и экономических структур* в соответствии с учебным планом

Форма обучения очная

Учебный год 2018/2019

Ответственный исполнитель

Доцент кафедры математического моделирования _____ Костин А.В____ 03.07.2018

должность, подразделение *подпись* *расшифровка подписи*

СОГЛАСОВАНО

Куратор ООП ВО

по направлению/ специальности _____ Костин В.А.._____ 03.07.2018

подпись *расшифровка подписи*

Начальник отдела

обслуживания ЗНБ _____ Васильченко Л.В._ 03.07.2018

подпись *расшифровка подписи*

Программа рекомендована НМС математического факультета

наименование факультета, структурного подразделения

протокол № 0500-07 от 03.07.2018 г.