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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа

А.Д. Баев
(подпись)
03.07.2018

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.02.02 Криптографические протоколы и стандарты
Код и наименование дисциплины в соответствии с Учебным планом

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

2. Профиль подготовки/специализации: Информационная безопасность финансовых и экономических структур

3. Квалификация (степень) выпускника: Специалист

4. Форма образования: Очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра математического анализа

6. Составители программы:
Залыгаева Марина Евгеньевна

7. **Рекомендована:** Научно-методическим Советом математического факультета протокол №0500-07 от 03.07.2018г.
(наименование рекомендующей структуры, дата, номер протокола)

8. Учебный год: 2018/2019 **Семестр(-ы):** 5

9. Цели и задачи учебной дисциплины:

Цели изучения дисциплины:

ознакомление студентов с существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области, формирование у них четкого представления и понимания теоретических и прикладных знаний о современных методах обеспечения аутентификации электронных документов в информационных инфраструктурах государственных и частнопредпринимательских предприятий и организаций.

Задачи дисциплины:

– обеспечить получение основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов;

– сформировать у студентов знания о фундаментальных алгебро-геометрических основах построения криптосистем, выработать знания и умения разбираться в закономерностях создания, использования и анализа современных криптопротоколов;

– выработать знания и умения применять полученные теоретические сведения для решения практических задач, в том числе в конкретной служебной деятельности правоохранительных органов;

– развить критический подход к решению задач с использованием криптографических протоколов через понимание отсутствия абсолютной защищенности распределенной информационной системы со многими участниками;

– ознакомить будущего специалиста с криптографическими протоколами, закрепленными национальными и международными стандартами.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Криптографические протоколы и стандарты» является дисциплиной по выбору вариативной части профессионального цикла Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по специальности 10.05.04 «Информационно-аналитические системы безопасности».

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 – 1	способность анализировать физические явления и процессы, а также применять соответствующий математический аппарат при решении задач в сфере профессиональной деятельности	знать**:** базовые принципы системного подхода и методов системного анализа, содержательное описание рассмотренных методов и примеров их применения при проектировании систем информационной безопасности и других сложных систем; роль и место методов и средств компьютерного имитационного моделирования при проектировании сложных систем, приемы и особенности их практического применения; этапы разработки компьютерных моделей систем, применяемые при этом технологии, а также гибридные математические схемы, используемые при построении моделей элементов систем и их взаимодействия. уметь**:** с использованием методов системного анализа проводить структурно-функциональный синтез систем обработки и защиты информации для реше-

		ния конкретных практических задач; формировать рекомендации по принципам построения и параметрам систем в конкретной предметной области, проводить разработку компьютерных моделей в интересах проведения анализа вариантов построения информационных, информационно-измерительных и систем информационной безопасности различного назначения, использовать основные способы алгоритмизации математических моделей систем, технологии организации и проведения имитационного эксперимента. владеть**:** практическими навыками применения методов и средств системного анализа; создания, планирования эксперимента и тестирования компьютерных моделей сложных систем
ПК – 7	способность проводить предпроектное обследование профессиональной деятельности и информационных потребностей автоматизируемых подразделений	знать**:** этапы разработки компьютерных моделей систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования, технологии организации и проведения статистического компьютерного моделирования компьютерных систем. уметь: анализировать адекватность модели и результаты модельного эксперимента, сопоставляя получаемые и планируемые результаты. владеть: практическими навыками применения средств и технологий; создания, планирования эксперимента и тестирования компьютерных моделей сложных систем (массового обслуживания, передачи информации, конфликтного взаимодействия систем).

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 3/108.
Форма промежуточной аттестации - экзамен

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)				
	Всего	По семестрам			
		5 сем.			
Аудиторные занятия	50	50			
в том числе: лекции	34	34			
практические	16	16			
лабораторные					
Самостоятельная работа	58	58			
Контрольные работы	1	1			
Итого:	108	108			

13.1 Содержание разделов дисциплины: 13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Понятие криптографического протокола	Понятие криптографического протокола. Отличия криптографического протокола от криптографического алгоритма. Общая классификация криптографических протоколов: протоколы с посредником, протоколы с арбитром, самодостаточные протоколы.

		Понятие атаки на криптографический протокол
1.2	Аутентификация и ключи	Основные соглашения об участниках криптографических протоколов. Основные соглашения о среде выполнения криптографических протоколов. Аутентификация источника данных и сущности. Генерация аутентифицированных ключей. Основные методы и механизмы аутентификации. Стратегия «окликотзыв». Механизм меток времени. Протоколы аутентификации. Аутентификация с помощью пароля. Протокол взаимоблокировки. Протокол Ву-Лама. Протокол Отвея-Рииса. Протоколы передачи сеансовых секретных ключей.
1.3	Криптографические стандарты	Обмен зашифрованными ключами EKE. Трехпроходный протокол Шамира. Протоколы предварительного распределения ключей. Протоколы совместной выработки общего ключа. Развитые протоколы обмена ключами с аутентификацией сторон. Типичные атаки на протоколы аутентификации. Протоколы защиты данных в сети Internet. Концепция криптографической защиты информации на сетевом уровне модели ISO/OSI. Депонирование ключей и возможность контроля информационного взаимодействия. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения. Алгоритмы генерации псевдослучайных последовательностей чисел. Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.
3 Лабораторные занятия		
1.1	Понятие криптографического протокола	Понятие криптографического протокола. Отличия криптографического протокола от криптографического алгоритма. Общая классификация криптографических протоколов: протоколы с посредником, протоколы с арбитром, самодостаточные протоколы. Понятие атаки на криптографический протокол
1.2	Аутентификация и ключи	Основные соглашения об участниках криптографических протоколов. Основные соглашения о среде выполнения криптографических протоколов. Аутентификация источника данных и сущности. Генерация аутентифицированных ключей. Основные методы и механизмы аутентификации. Стратегия «окликотзыв». Механизм меток времени. Протоколы аутентификации. Аутентификация с помощью пароля. Протокол взаимоблокировки. Протокол Ву-Лама. Протокол Отвея-Рииса. Протоколы передачи сеансовых секретных ключей.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Понятие криптографического протокола	10		6	16	16
02	Аутентификация и ключи	6		8	19	38
03	Криптографические стандарты	6		3	19	48

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.)
Перечень вопросов, содержащихся в рабочей программе дисциплины, может быть изложен с различной степенью глубины в соответствии с объемом часов на самостоятельную работу студентов.

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

а) основная литература:

№ п/п	Источник
1	Новикова Н. М. Прикладная математическая статистика: учебное пособие / Н.М. Новикова, С.Л. Подвальный. — Воронеж : Воронежский государственный технический университет, 2013. Ч.2 -179 с.
2	Костенко И. П. Вероятность и статистика : курс лекций и упражнений / И.П. Костенко .— Москва ; Ижевск : Регулярная и хаотическая динамика, 2012 .— 380 с
3	Теория риска [Электронный ресурс] : учебно-методическое пособие : [для студ. 3-5 к. очной формы обучения специальности 010101 - Математика] / Воронеж. гос. ун-т ; сост. И.В. Михайлова .— Электрон. текстовые дан. — Воронеж : ИПЦ ВГУ, 2011 .— Загл. с титул. экрана .— Электрон. версия печ. публикации .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— Windows 2000 ; Adobe Acrobat Reader.
4	Алгазинов, Эдуарт Константинович. Анализ и компьютерное моделирование информационных процессов и систем : [учебное пособие для студ. вузов, обуч. по специальности 080801 "Приклад. информатика" и др. междисциплинар. специальностям] / Э.К. Алгазинов, А.А. Сирота ; под общ. ред. А.А. Сироты .— М. : Диалог-МИФИ, 2009 .— 416 с. : ил .— Библиогр. в конце разд. — ISBN 978-5-86404-233-5

б) дополнительная литература:

№ п/п	Источник
1	Сирота А.А. Компьютерное моделирование и оценка эффективности сложных систем.– М.: Техносфера, 2006, 256 с.
2	Фалин А.И Актуарная математика в задачах / Г.И. Фалин, А.И. Фалин. - М.: Физматлит, 2003 .— 190 с..
3	Практикум по курсу "Моделирование систем" [Электронный ресурс] : учебно-методическое пособие для вузов : [для студ. 4-5 курсов фак. компьютер. наук днев. и вечер. формы обучения; для направлений: 230200 - Информ. системы, 230400 - Информ. системы и технологии; специальности, 230201 - Информ. системы и технологии]. Ч. 1,2 / Воронеж. гос. ун-т ; сост.: А.А. Сирота, Е.Ю. Митрофанова , М.А. Дрюченко .— Электрон. текстовые дан. — Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2013

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

№ п/п	Источник
4	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)
5	http://www.machinelearning.ru/ - профессиональный информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных

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

№ п/п	Источник
6	Практикум по курсу "Моделирование систем" [Электронный ресурс] : учебно-методическое пособие для вузов : [для студ. 4-5 курсов фак. компьютер. наук днев. и вечер. формы обу- чения; для направлений: 230200 - Информ. системы, 230400 - Информ. системы и техно- логии; специальности, 230201 - Информ. системы и технологии]. Ч. 1,2 / Воронеж. гос. ун-т ; сост.: А.А. Сирота, Е.Ю. Митрофанова , М.А. Дрюченко .— Электрон. текстовые дан. — Воронеж : Издательско-полиграфический центр Воронежского государственного университе- тета, 2013
7	Алгазинов, Эдуарт Константинович. Анализ и компьютерное моделирование информаци- онных процессов и систем : [учебное пособие для студ. вузов, обуч. по специальности 080801 "Приклад. информатика" и др. междисциплинар. специальностям] / Э.К. Алгазинов, А.А. Сирота ; под общ. ред. А.А. Сироты .— М. : Диалог-МИФИ, 2009 .— 416 с. : ил .— Библиогр. в конце разд. — ISBN 978-5-86404-233-5

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

18. Материально-техническое обеспечение дисциплины:

Доска, мел, тряпка, учебные пособия, компьютер

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	знать: терминологию прогнозирования; виды моделей и методов, используемых для прогнозирования в экономике, области их применения; программные продукты, которые используют для разработки прогнозов; место задач прогнозирования в информационно- аналитических системах, опыт их решения в подобных системах; отечественный и зарубежный опыт использования методов прогнозиро-	Раздел 1.	

	вания		
	уметь: выбирать модель/метод прогнозирования на основе качественного анализа объекта исследования; строить на основе описания ситуаций модели прогнозирования; оценивать качество построенных моделей с точки зрения их адекватности фактическим данным; прогнозировать на основе построенных моделей поведение экономических агентов, развитие экономических процессов и явлений, представлять результаты работы в виде выступления, аналитического отчета;	Раздел 2	
	владеть (иметь навык(и)): навыками спецификации и идентификации моделей прогнозирования; навыками построения моделей прогнозирования с использованием современных программных продуктов; навыками самостоятельной работы по организации и проведению процесса прогнозирования	Раздел 4.	Контрольная работа
Промежуточная аттестация			КИМ

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

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет теоретическими основами дисциплины, способен иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения практических задач в области теории прогнозирования	Повышенный уровень	Отлично
Обучающийся владеет теоретическими основами дисциплины, допускает ошибки при ответе на дополнительные вопросы, которые исправляет при помощи преподавателя	Базовый уровень	Хорошо
Обучающийся владеет частично теоретическими основами дисциплины, фрагментарно способен отве-	Пороговый	Удовлетво-

чать на дополнительные вопросы, не умеет применять теорию к практике.	уровень	рительно
Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки при ответе на основные и дополнительные вопросы	–	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 экзамену:

№	
1	Математические описания систем и моделей систем в рамках теоретико-множественного подхода.
2	Системы и проблемы. Системный подход и системный анализ. Качественные и количественные методы.
3	Общая методика системного анализа применительно к проектированию информационных и информационно-измерительных систем.
4	Задачи анализа и синтеза систем. Эволюционная технологическая схема синтеза сложных систем.
5	Метод анализа иерархий. Технология структурирования целей при разработке системы. Использование МАИ на начальной стадии разработки системы.
6	Морфологические методы и генерация альтернативных вариантов системы.
7	Современные информационно-аналитические технологии структурного системного анализа.
8	Объектно-ориентированный анализ и моделирование систем.
9	Обоснование структуры трехрубежной системы информационной безопасности организации.
10	Типовые математические схемы элементов сложной системы
11	Комбинированный подход. Математическая схема агрегата. Гибридные автоматы.
12	Метод статистических испытаний Монте-Карло. Способы организации модельного времени и квазипараллелизма имитационной модели.
13	Моделирование случайных величин с заданным законом распределения. Датчики случайных чисел.
14	Моделирование случайных величин с произвольным законом распределения.
15	Языки и инструментальные средства имитационного моделирования.
16	Принципы моделирования информационного конфликта систем.

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 и контрольной 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 практическое задание, позволяющее оценить степень сформированности умений и навыков.

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