МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины

Математические методы защиты банковской информации

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью курса «Математические методы защиты банковской информации» (ММЗБИ) является ознакомление студентов с основополагающими принципами защиты информации с помощью криптографических методов и примерами реализации этих методов на практике. Содействие формированию практических навыков построения систем защиты информации, применение математических методов в информационной безопасности электронного бизнеса.

2. Место дисциплины в структуре ОП специалитета

Данная дисциплина является дисциплиной по выбору. Она является частью ядра образования в системе обучения методам криптографической информации, состоящего из дисциплин «Криптографические методы защиты информации», «Теоретико-числовые методы в криптографии», «Программно-аппаратные средства обеспечения безопасности», «Криптографические протоколы». Изучение дисциплины базируется также на курсах «Алгебра», «Теория вероятностей», «Теория чисел».

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП специалитета

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК - 10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	**И-ОПК-10.1.** Понимать корректность криптографической алгоритмов в современных программных комплексах. **И-ОПК-10.2.** Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. **И-ОПК-10.3.** Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	Знать: -основные задачи, решаемые криптографическими методами; -зарубежные и российские криптографические стандарты; -механизмы реализации атак в сетях **Уметь:** - корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; -осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; **Владеть:** -навыками работы с научно-технической литературой по тематике дисциплины.

4. Объем, структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа						
			лекции	практические	Лабораторные	Консультации	аттестационные испытания	самостоятельная работа	
1	Введение	10	2						
2	Особенности применения криптографии в банковском деле	10	4	8		2		8	Задания для самостоятельной работы, контрольная работа № 1
3	Системы электронных платежей. Классификация и структура СЭП	10	8	8				8	
4	Криптографические протоколы в электронной коммерции	10	8	8		2		8	Задания для самостоятельной работы, контрольная работа № 2
5	Банковские криптографические протоколы	10	10	8		2		8	Задания для самостоятельной работы, контрольная работа № 3
							0,3	5,7	зачет
	Всего		32	32		6	0,3	37,7	108

Содержание разделов дисциплины

1. Введение

Средства и системы криптографической защиты информации играют важную роль в современных компьютерных системах, используемых в сфере финансовой деятельности. Интерес к ним обусловлен не только возрастающими общественными потребностями в переводе экономических отношений на «электронную основу», но и сильно расширившимися возможностями передачи, обработки и хранения информации в распределенных вычислительных системах.

2. Особенности применения криптографии в банковском деле

Характеристика платежной системы России. Угрозы безопасности информации в платежной системе. Проблемы криптографической защиты платежной системы. Критерии и требования к криптографическим средствам защиты банковской информации. Новые направления, стимулируемые банковскими приложениями.

3. Системы электронных платежей. Классификация и структура СЭП

Потребительские качества СЭП. Неанонимные СЭП, работающие в реальном масштабе времени. Неанонимные автономные СЭП. Анонимные СЭП, работающие в реальном масштабе времени. СЭП на базе затемненной подписи. СЭП, основанные на взломозащищенных устройствах, СЭП с идентификацией повторной траты монеты.

4. Криптографические протоколы в электронной коммерции

Основные задачи защиты информации в электронной коммерции. Защищенные каналы передачи информации. Честный обмен цифровыми подписями и его приложения. Честный обмен цифровыми данными.

5. Банковские криптографические протоколы

Общая схема. Схема Якоби. Схемы Шаума. Схема Брандса.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Академическая лекция, как правило, состоит из трех частей: вступления (введения), изложения и заключения:

вступление (введение) определяет тему, план и цель лекции. Оно призвано заинтересовать и настроить аудиторию, сообщить, в чём заключается предмет лекции и (или) её актуальность, основная идея (проблема, центральный вопрос), связь с предыдущими и последующими занятиями, поставить её основные вопросы. Введение должно быть кратким и целенаправленным.

изложение является основной частью лекции, в которой реализуется научное содержание темы, ставятся все узловые вопросы, приводится вся система доказательств с использованием наиболее целесообразных методических приемов. Каждое теоретическое положение должно быть обосновано и доказано, приводимые формулировки и определения должны быть четкими, насыщенными глубоким содержанием.

Заключение обобщает в кратких формулировках основные идеи лекции, логически ее завершая. В заключении могут даваться рекомендации о порядке дальнейшего изучения основных вопросов лекции самостоятельно по указанной литературе.

Лекция с разбором конкретных ситуаций – это по форме та же лекция - дискуссия, но на обсуждение преподаватель ставит не вопрос, а конкретную ситуацию. Как правило, такая ситуация представляется устно или в очень короткой видеозаписи, поэтому изложение ее должно быть очень кратким, но содержать достаточную информацию для оценки характерного явления и обсуждения. Это, так называемая, микроситуация. Слушатели анализируют и обсуждают ее сообща, всей аудиторией. Преподаватель старается активизировать участие в обсуждении отдельными вопросами, обращенными к отдельным слушателям, выясняет их оценку суждениям коллег, предлагает сопоставить с собственной практикой, «сталкивает» между собой различные мнения и тем развивает дискуссию, стремясь направить ее в нужное русло. Затем, опираясь на правильные высказывания и анализируя неправильные, ненавязчиво, но убедительно подводит аудиторию к коллективному выводу или обобщению.

Обобщающая лекция – проводится в завершение изучения раздела или темы для закрепления знаний. На лекции вновь выделяются основные вопросы, используются обобщающие таблицы, схемы, алгоритмы, позволяющие включить усвоенные знания в новые связи и зависимости, переводя их на более высокие уровни усвоения.

Обзорная лекция – проводится обычно перед государственными или курсовыми экзаменами. В лекции излагаются лишь отдельные, наиболее крупные вопросы дисциплины. Материал лекции представляет конспективный обзор полного учебного курса. Проводится такая лекция с целью систематизации знаний студентов, полученных ими в ходе изучения (в том числе самостоятельного) учебного материала.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний по предложенному алгоритму.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)

В процессе осуществления образовательного процесса используются:
-программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов: Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);
- Microsoft OfficeSTD 2013;
- MikTeX (свободно распространяемое ПО).

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490278 (дата обращения: 24.01.2022).
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный //

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262 (дата обращения: 24.01.2022).

б) дополнительная литература

1. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 24.01.2022). — Режим доступа: для авториз. пользователей.
2. Сковиков, А. Г. Цифровая экономика. Электронный бизнес и электронная коммерция : учебное пособие для вузов / А. Г. Сковиков. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 260 с. — ISBN 978-5-8114-9249-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189400 (дата обращения: 24.01.2022). — Режим доступа: для авториз. пользователей.

б) ресурсы сети «Интернет»:

1. Электронный каталог Научной библиотеки ЯрГУ (https://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).
2. Электронная библиотечная система (ЭБС) издательства «Юрайт» (https://www.urait.ru).
3. Электронная библиотечная система (ЭБС) издательства «Проспект» (http://ebs.prospekt.org/).
4. Научная электронная библиотека (НЭБ) (http://elibrary.ru)

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

-учебные аудитории для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;

-помещения для самостоятельной работы;

-помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в аудитории для практических занятий больше либо равно списочному составу группы обучающихся.

Составитель Зеткина О.В.. доцент, к.э.н.

Приложение №1 к рабочей программе дисциплины
«Математические методы защиты банковской информации»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1. Контрольные задания и иные материалы. Задания для самостоятельной работы, используемые в процессе текущей аттестации (И-ОПК-10.1, И-ОПК-10.2, И-ОПК-10.3)

Задания по теме «Особенности применения криптографии в банковском деле»

Характеристика платежной системы России. Виды угроз безопасности информации в платежной системе. Критерии и требования к криптографическим средствам защиты банковской информации.

Задания по теме «Системы электронных платежей. Классификация и структура СЭП».

Модельное представление СЭП. Системы наличных платежей. Системы денежных переводов. Потребительские качества СЭП. Три вида решения проблемы повторной траты монеты. Неанонимные СЭП, работающие в реальном масштабе времени. Системы без криптографической защиты. Системы с симметричной аутентификацией. Неанонимные автономные СЭП. Системы на основе цифровой подписи. Анонимные СЭП. СЭП на базе затемненной подписи.

Задания по теме «Криптографические протоколы в электронной коммерции»

Защищенные каналы передачи информации. Принцип туннелирования протоколов. Использования протокола AH. Протокол ESP. Спецификация SSL / TLS. Честный обмен цифровыми подписями. Честный обмен цифровыми данными.

Задания по теме «Банковские криптографические протоколы»

Схемы Шаума. Доказуемо стойкие схемы. Схема Якоби, Схема Брандса.

Контрольная работа № 1(И-ОПК-10.1)

1. Какие виды цифровой подписи с дополнительной функциональностью используются в СЭП и для каких целей.
2. Приведите примеры ситуаций, когда анонимность и неотслеживаемость в СЭП могут быть утрачены по причинам, не связанными непосредственно с особенностями применения криптографических алгоритмов и протоколов.
3. С какой целью в СЭП Шаума могут вводиться ключи монет?
4. Каким образом в СЭП Брандса в «электронных монетах» кодируются идентификаторы плательщиков?

Контрольная работа № 2(И-ОПК-10.2)

1. Назовите два класса задач, возникающих при дистанционном осуществлении коммерческих отношений.
2. Какие уровни информационного взаимодействия удобно выделить в электронной коммерции?
3. Назовите три основных вида информационных объектов, рассматриваемые в электронной коммерции. Какие задачи защиты информации порождает необходимость обмена этими объектами?

Контрольная работа № 3 (И-ОПК-10.3)

1. Что принято понимать под защищенным каналом передачи данных?
2. Назовите известные вам задачи электронной коммерции, которые можно решить криптографическими методами на основе схемы честного обмена цифровыми подписями.
3. Перечислите классы угроз информационной безопасности в банковском деле.

Оценивание результатов выполнения контрольных работ

1) Проведение контрольных работ осуществляется с целью проверки уровня знаний, владений, понимания студентом основных вопросов, методов и законов изучаемой теории.
2) **Правила выставления оценки:**
3) «отлично» - студент полностью ответил на все вопросы, поставленные в контрольной работе, обосновав их ссылками на изученный материал.
4) «хорошо» - студент ответил на поставленные вопросы, но в обосновании имеются сомнения;
5) «удовлетворительно» - студент ответил на часть вопросов при неполном использовании понятийного аппарата дисциплины;
6) «неудовлетворительно» - студент не смог ответить на вопросы, поставленные в контрольной работе.

1.2. Список вопросов и (или) заданий для проведения промежуточной аттестации
Вопросы к зачету (И-ОПК-10.1, И-ОПК-10.2, И-ОПК-10.3)

1. Особенности информационной безопасности банковских и платежных систем.
2. Безопасность электронных платежей. Электронные платежи в банке.
3. Вопросы безопасности электронных платежей. Методы защиты в платежных и банковских системах.
4. Криптографические методы защиты информации.
5. Оценка надежности криптоалгоритмов.
6. Классификация методов шифрования информации. Абсолютно стойкий шифр.
7. Гаммирование Поточные шифры Идентификация и проверка подлинности.
8. Основные понятия и концепции. Особенности применения пароля для аутентификации пользователя.
9. Взаимная проверка подлинности пользователей Протоколы идентификации с нулевой передачей знаний.
10. Упрощенная схема идентификации с нулевой передачей знаний. Схема идентификации Гиллоу-Куискуотера.
11. Электронная цифровая подпись. Проблема аутентификации данных и электронная цифровая подпись.

12. Алгоритмы электронной цифровой подписи. Алгоритм цифровой подписи RSA.
13. Отечественный стандарт цифровой подписи.
14. Три вида решения проблемы повторной траты монеты.
15. Неанонимные автономные СЭП.
16. Что принято понимать под защищенным каналом передачи данных?

– .

Описание процедуры выставления оценки

Оценка ответа на зачете в значительной степени зависит от работы студента в течение семестра.

Оценка «**зачтено»** ставится в случае, если выполняются 2 условия:

1) студент ответил на зачете на оценку, составляющую *не менее 60%* от максимально возможного количества баллов (6 баллов из 10).

2) студент выполнил тесты *не ниже, чем на оценку «удовлетворительно»* (схема выставления оценки по тестам приведена выше в настоящей Программе).

Баллы по ответу на зачете

Минимальный порог 6 баллов из 10.

- 10 баллов выставляется за полный ответ на поставленный вопрос с включением в содержание ответа лекции, материалов учебников, дополнительной литературы без наводящих вопросов.

- 8-9 баллов выставляется за полный ответ на поставленный вопрос в объеме лекции с включением в содержание ответа материалов учебников с четкими ответами на наводящие вопросы преподавателя.

-6-7 баллов выставляется за ответ, в котором озвучено более половины требуемого материала, с положительным ответом на большую часть наводящих вопросов.

Оценка «**не зачтено»** ставится в случае, если выполняется хотя бы одно из условий:

1)студент ответил на зачете на оценку, составляющую *50% и меньше* от максимально возможного количества баллов (5 и меньше баллов из 10).

2) студент выполнил тесты *ниже, чем на оценку «удовлетворительно»* (схема выставления оценки по тестам приведена выше в настоящей Программе).

5 и менее баллов выставляется за ответ, в котором озвучено менее половины требуемого материала, не озвучено главное в содержании вопроса с отрицательными ответами на наводящие вопросы или студент отказался от ответа без предварительного объяснения уважительных причин.

Приложение №2 к рабочей программе дисциплины
«Математические методы защиты банковской информации»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Математические методы защиты банковской информации» являются лекции. По большинству тем предусмотрены практические занятия.

Для успешного освоения дисциплины очень важно решение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях и более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы в течение обучения проводятся мероприятия текущей аттестации в виде контрольных работ. Также проводятся консультации по разбору заданий для самостоятельной работы, которые вызвали затруднения.

В конце семестра изучения дисциплины студенты сдают зачет.

Освоить вопросы, излагаемые в процессе изучения дисциплины, самостоятельно студенту крайне сложно. Это связано со сложностью изучаемого материала. Поэтому высокий уровень посещения аудиторных занятий является необходимым.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы рекомендуется использовать учебную литературу:

а) основная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490278 (дата обращения: 24.01.2022).
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262 (дата обращения: 24.01.2022).

б) дополнительная литература

3. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/book/156401 (дата обращения: 24.01.2022). — Режим доступа: для авториз. пользователей.

4. Сковиков, А. Г. Цифровая экономика. Электронный бизнес и электронная коммерция : учебное пособие для вузов / А. Г. Сковиков. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 260 с. — ISBN 978-5-8114-9249-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189400 (дата обращения: 24.01.2022). — Режим доступа: для авториз. пользователей.

б) ресурсы сети «Интернет»:

5. Электронный каталог Научной библиотеки ЯрГУ (https://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).
6. Электронная библиотечная система (ЭБС) издательства «Юрайт» (https://www.urait.ru).
7. Электронная библиотечная система (ЭБС) издательства «Проспект» (http://ebs.prospekt.org/).
8. Научная электронная библиотека (НЭБ) (http://elibrary.ru)