

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе

И.Б. Поверинов

31 августа 2017 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ФИНАНСОВАЯ КРИПТОГРАФИЯ»

Направление подготовки 10.03.01 – Информационная безопасность

Квалификация (степень) выпускника Бакалавр


Профиль (направленность) Информационно-аналитические системы финансового мониторинга

Академический бакалавриат

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки 01.12.2016 г. №1515

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Профессор, доктор физ.-мат. наук  И.Т. Артемьев

ОБСУЖДЕНО:

на заседании кафедры математического и аппаратного обеспечения информационных систем 30.08.2017 г., протокол № 1

заведующий кафедрой

СОГЛАСОВАНО:

 Д.В. Ильин

Методическая комиссия факультета информатики и вычислительной техники 30 августа 2017 г., протокол №1


Декан факультета


Директор научной библиотеки

Начальник управления информатизации

Начальник учебно-методического управления

 А.В. Щипцова

 Н. Д. Никитина

 И. П. Пивоваров

 В. И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине	4
2. Место дисциплины в структуре основной образовательной программы (ООП)	4
3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП	4
4. Структура и содержание дисциплины	5
5. Содержание разделов дисциплины	6
6. Образовательные технологии	7
7. Формы аттестации и оценочные материалы	8
8. Учебно-методическое и информационное обеспечение дисциплины	9
9. Материально-техническое обеспечение дисциплины	11
10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями	11
11. Методические рекомендации по освоению дисциплины	11

1. Цель и задачи обучения по дисциплине

Цель дисциплины изучение методов организации защиты проведения электронных финансовых сделок (транзакций), изучить применяемые протоколы и криптошифры. Уметь программно реализовать вышеупомянутые методики. Студенты должны знать основные угрозы безопасности финансовых систем и способы обнаружения, предотвращения и устранения таких угроз, иметь понятие по проблемам безопасности в системах коллективного хранения финансовой информации, а также угроз, существующих при использовании телекоммуникационных технологий для проведения транзакций.

Задачами курса являются освоение технологий диагностики опасностей и угроз для финансовых операций(транзакций). Разбираются основные методы криптографической защиты информации, типы угроз и способы парирования таких угроз. Студенты обучаются технологиям создания защищенных сред, криптографического шифрования и методам стеганографии в области финансов, технологии электронной подписи и коллективного хранения информации. Также уделяется внимание аспекту комфортности и надежности при использовании криптографических средств.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина относится к дисциплинам по выбору вариативной части образовательной программы по направлению 10.03.01 Информационная безопасность (профиль Информационно-аналитические системы финансового мониторинга).

Базируется на знаниях, умениях и навыках полученных в процессе изучения дисциплин «Криптографические методы защиты информации», «Экономика», «Криптографические протоколы и стандарты».

Является предшествующей для преддипломной практики, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

ПК-2 – способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

ПК-7 - способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

- понятие финансов и финансовых операций (транзакций) (31);
- методы защиты информации при проведении финансовых операций (32);
- стандартизация и сертификация криптографических методов в области финансовых операций (33);
- возможные угрозы, исходящие от сторонних лиц при использовании телекоммуникационных каналов, методы атак и противодействие им (34);
- определение и проверка достоверности квалифицированной электронной подписи (35);
- методы группового хранения финансовой информации (36),
- основные положения законодательства в области проведения финансовых операций с криптовалютами (37).

уметь:

- использовать программные и технические средства защиты при проведении транзакций (У1);

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Введение в финансовую криптографию.								
1.1. Финансы и криптография.	4	2	2				2	
Раздел 2. Комфортность использования криптографических средств.								
2.1. Защищенная среда выполнения (цели, принципы, методы создания).	4	2				2	2	
2.2. Комфортность использования криптографических средств.	10	2				8		
Раздел 3. Криптографические методы в области финансов.								
3.1. История использования криптографии в финансовых взаимоотношениях.	4	2	2				2	
3.2. UML диаграммы, рассмотрение криптошифров с помощью UML диаграмм.	10	2	2			6	2	
Раздел 4. Криптоанализ.								
4.1. Изучение идентифицирующих токенов на примере cookie.	3	1	2				2	
4.2. Рассмотрение методов криптоанализа применительно к финансовым криптошифрам и протоколам.	17	1	4			12	2	
Раздел 5. Криптовалюты.								
5.1. Технология блокчейн.	6	2	2			2	2	
5.2. Цифровые подписи блоков.	5	1	2			2		
5.3. Технологии криптовалютных транзакций. Майнинг криптовалют, функционирование криптовалютных бирж.	7	1				6	2	
Зачет	2				2			
Итого	72 2 з.е.	16	16		2	38	16	

5. Содержание разделов дисциплины

5.1. Лекции

Раздел 1. Введение в финансовую криптографию.

Л 1.1. Финансы и криптография.

Раздел 2. Комфортность использования криптографических средств.

Л 2.1. Защищенная среда выполнения(цели, принципы, методы создания).

Л 2.2. Комфортность использования криптографических средств.

СРС – Доклад: рассмотрение комфортности отдельных криптографических средств.

Раздел 3. Криптографические методы в области финансов.

3.1. История использования криптографии в финансовых взаимоотношениях.

3.2. UML диаграммы, рассмотрение криптошифров с помощью UML диаграмм.

Раздел 4. Криптоанализ.

4.1. Изучение идентифицирующих токенов на примере cookie.

4.2. Рассмотрение методов криптоанализа применительно к финансовым криптошифрам и протоколам.

Раздел 5. Криптовалюты.

5.1. Технология блокчейн.

5.2. Цифровые подписи блоков

5.3. Технологии криптовалютных транзакций. Майнинг криптовалют, функционирование криптовалютных бирж.

5.2. Лабораторные работы

п/п	Название	Раздел	Кол-во часов
1.	Решение задач по криптографии	1.1. Финансы и криптография.	2
2.	Протокол «рукопожатие» и защищенный обмен информацией по открытым каналам	3.1. История использования криптографии в финансовых взаимоотношениях.	2
3.	Построение диаграммы протокола «рукопожатие» или криптошифра.	3.2. UML диаграммы, рассмотрение криптошифров с помощью UML диаграмм.	2
4.	Моделирование перехвата идентифицирующих cookie	4.1. Изучение идентифицирующих токенов на примере cookie.	2
5.	Оценка математического ожидания времени взлома в зависимости от вариативности брутфорса	4.2. Рассмотрение методов криптоанализа применительно к финансовым криптошифрам и протоколам.	4
6.	Внедрение сервисов ЭДО в программное обеспечение	5.2. Цифровые подписи блоков.	2
7.	Изучение open source программ биткоин кошельков, установка и извлечение подписей блоков, расчет конечного состояния кошелька	5.3. Технологии криптовалютных транзакций. Майнинг криптовалют, функционирование криптовалютных бирж.	2

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

- диагностики;
- целеполагания;
- управления процессом освоения учебной информации;
- применения знаний на практике, поиска новой учебной информации;
- организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.);
- контроля качества и оценивания результатов образовательной деятельности (технология оценивания качества знаний, рейтинговая технология оценки знаний и др.)

В соответствии с требованиями ФГОС ВО для реализации компетентного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

- лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;
- лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования,

направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: анализ, аннотирование и конспектирование литературы по теме, подготовка к лабораторным работам, подготовка реферативных сообщений, подготовка тезисов к дискуссии, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчетов по результатам выполненных заданий и лабораторных работ, решений задач и ситуаций; защита исследовательской работы. Результаты самостоятельной работы учитываются при оценке знаний на зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Принимается зачет преподавателем, читающим лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся:

7.1. Вопросы к зачету

1. Дайте определение термину «Финансы».
2. Дайте определение термину «Финансовые операции (транзакции)».
3. Роль криптографии в области финансов.
4. Дайте определение термину «Программные и техническим криптографические средства защиты информации», что к ним относится?
5. Дайте определение термину «Комфортность» программных и технических средств.
6. Каковы методы защиты информации при проведении финансовых операций.
7. Стандартизация и сертификация криптографических методов в области финансовых операций.
8. Каковы отличия UML диаграмм от блоковых диаграмм.
9. Этапы тестирования криптографических средств, какие виды диаграмм возможно применять на каждом этапе.
10. Опишите протокол «рукопожатие» и процесс обмена сертификатами.
11. Дайте характеристики ролям(актерам – Алиса, Боб, Дэвид, Чак), используемым в протоколах защищенного обмена по открытым каналам. Опишите степень возможных угроз их действий (бездействия) при организации защищенного обмена информацией по открытым каналам.
12. Опишите методы проведения криптоанализа, как злоумышленник реализует данные методы.
13. Опишите методы атак на транзакции, реализуемые злоумышленником без использования методов криптоанализа.
14. Назовите основные методы противодействия атакам злоумышленника(-ов) при проведении транзакций.
15. Дайте определение термину электронная подпись квалифицированная(электронная цифровая подпись).

16. Как реализуется защита электронной подписи от подделки злоумышленником.
17. Как реализуется проверка достоверности электронной подписи (технология PKI)
18. Как производится подписание документа электронной подписью, назовите известные сервисы электронного документооборота.
19. Дайте общее описание отличий электронной подписи и специализированных приложений электронной подписи, форматы электронных документов.
20. Дайте понятие методу группового хранения финансовой информации, какова роль технологии блокчейн при хранении базы данных транзакций.
21. Методики формирования и подписания блоков в распределенной базе, методы ускорения проведения транзакций в технологии блокчейн.
22. Законодательство в области проведения финансовых операций с криптовалютами в мире и в Российской Федерации.
23. Дайте описание термину «Криптовалюта», каковы отличия эмиссии и обеспечения от эмитированных государственных финансовых инструментов.
24. Роль майнеров криптовалют при проведении криптовалютных транзакций.
25. Дайте описание понятию «Криптовалютная биржа», какова роль организаторов, организация кроссбиржевой торговли криптовалютами.

Зачет проводится по окончании занятий по дисциплине до начала экзаменационной сессии в период недели контроля самостоятельной работы.

Билет для проведения промежуточной аттестации в форме зачета включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания и лабораторные работы в течение семестра, чей уровень знаний, умений и навыков соответствует уровню оценок «отлично», «хорошо» или «удовлетворительно». Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания и лабораторные работы в течение семестра, либо чей уровень знаний, умений и навыков соответствует уровню оценки «неудовлетворительно».

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке <http://library.chuvsu.ru/>

8.1. Рекомендуемая основная литература (ежегодное обновление перечня и условия доступа представлены в Приложениях к рабочей программе)

№ п/п	Наименование
1.	Бескид П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс] : учебное пособие / П.П. Бескид, Т.М. Тагарникова. — Электрон. текстовые данные. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 95 с. Режим доступа: http://www.iprbookshop.ru/17925.html
2.	Аграновский А.В. Практическая криптография. Алгоритмы и их программирование [Электронный ресурс] / А.В. Аграновский, Р.А. Хади. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2009. — 256 с. Режим доступа: http://www.iprbookshop.ru/8641.html
3.	Земор Ж. Курс криптографии [Электронный ресурс] / Ж. Земор. — Электрон. текстовые данные. — Москва, Ижевск: Регулярная и хаотическая динамика, Ижевский институт компьютерных исследований, 2006. — 256 Режим доступа: http://www.iprbookshop.ru/16547.html

8.2. Рекомендуемая дополнительная литература (ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе)

№ п/п	Наименование
1.	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М. : Издательство Юрайт, 2017. — 209 с. Режим доступа : www.biblio-online.ru/book/C0328DC2-2A46-4945-994F-04F661095B83 .
2.	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М. : Издательство Юрайт, 2017. — 245 с. Режим доступа : www.biblio-online.ru/book/AF99BBDE-AF3A-43A9-A90F-B99806553C25
3.	Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях [Электронный ресурс] : практическое пособие / С.И. Алешников, Е.В. Козьминых. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2006. — 97 с. Режим доступа: http://www.iprbookshop.ru/23851.html
4.	Гульятеева Т.А. Основы теории информации и криптографии [Электронный ресурс] : конспект лекций / Т.А. Гульятеева. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2010. — 88 с. Режим доступа: http://www.iprbookshop.ru/44987.html
5.	Басалова Г.В. Основы криптографии [Электронный ресурс] / Г.В. Басалова. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 282 с. Режим доступа: http://www.iprbookshop.ru/52158.html

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке <http://ui.chuvsu.ru/>*

8.3.1. Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
2.	MS Windows/Linux (Ubuntu)	лицензия университета/ свободное лицензионное соглашение (http://ubuntu.ru/)
3.	Демо версия КриптоАРМ	https://www.trusted.ru/products/cryptoarm/about/
4.	КриптоПро УЦ 2	https://www.cryptopro.ru/products/ca/2.0
5.	HTTP Analyzer 7	http://www.ieinspector.com/httpanalyzer/download.html
6.	Visual Paradigm Community Edition	https://www.visual-paradigm.com/download/community.jsp

8.3.2. Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.3.3. Рекомендуемые интернет-ресурсы и открытые он-лайн курсы

№ п/п	Наименование интернет ресурса	Режим доступа
1.	Российская Государственная Библиотека	http://www.rsl.ru
2.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
3.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
4.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
5.	Научная электронная библиотека	http://elibrary.ru
6.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
7.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

- ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);
- мультимедийный проектор с дистанционным управлением;
- мультимедийное звуковое оборудование;
- настенный экран;
- интерактивная доска SMART;
- телевизор SMART.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки,

раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Формы организации студентов на лабораторных работах: фронтальная, групповая и индивидуальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек. При индивидуальной форме организации занятий каждый студент выполняет индивидуальное задание.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.