

Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

БЛОКЧЕЙН

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:

Разработка защищенных телекоммуникационных систем

Квалификация:

Специалист

Форма обучения

Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность
телекоммуникационных систем»



Татарникова Т.М.

Утверждаю

Председатель УМС  И.И. Палкин

Рекомендована решением

Учебно-методического совета

«22» сентября 2020 г., протокол № 1

Рассмотрена и утверждена на заседании кафедры

«31» августа 2020 г., протокол № 8

Зав. кафедрой  Т.М. Татарникова

Авторы-разработчики:



Татарникова Т.М.

Санкт-Петербург 2020

Цели освоения дисциплины

Целью освоения дисциплины «Блокчейн» является формирование знаний, позволяющих использовать соответствующий математический аппарат и инструментальные средства создания и применения блокчейн в инфокоммуникационных технологиях, составляющих основу цифровой экономики.

Задачи дисциплины:

- изучение специальной терминологии технологии распределенных реестров (блокчейн);
- изучение технологий создания и применения блокчейн.

1. Место дисциплины в структуре ОП

Дисциплина «Блокчейн» для специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» относится к дисциплинам по выбору (шифр Б1.В.ДВ.03.02).

Для освоения дисциплины «Блокчейн», необходимо освоить учебный материал предшествующих дисциплин:

- «Информационные технологии»;
- «Защищенный документооборот»;
- «Дискретная математика».

Параллельно с дисциплиной «Блокчейн» изучаются дисциплины: «Защита операционных систем», «Сети и системы передачи информации» и является предшествующей для дисциплин: «Информационно-аналитические системы», «Защищенные корпоративные сети».

Знания и практики, полученные обучаемыми по дисциплине «Блокчейн», непосредственно используются для подготовки выпускной квалификационной работы и в практической профессиональной деятельности, связанной с организацией надежного учета различных активов.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Компетенция
ОПК-5	способностью применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач
ПК-7	способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования
ПК-14	способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем

В результате освоения компетенций в рамках дисциплины «Блокчейн» обучающийся должен:

Код компетенции	Результаты обучения
ОПК-5	Знать: области и особенности использования смарт-контрактов; Уметь: использовать технологии блокчейн в целях разработки и реализации новых программных продуктов и услуг; Владеть: методами и приемами применения блокчейн
ПК-7	Знать: сильные и слабые стороны технологий блокчейн; Уметь: оценить потенциальные риски и перспективы проектов блокчейн; Владеть: методами оценки эффективности использования технологий блокчейн
ПК-14	Знать: математические и технические основы блокчейн; Уметь: проектировать блокчейн-приложение; Владеть: базовыми навыками работы на платформах блокчейн.

Основные признаки проявленности формируемых компетенций в результате освоения дисциплины «Блокчейн» сведены в таблице.

Уровень освоения компетенции	Результат обучения	Результат обучения	Результат обучения
	ОПК-5: Знать, уметь, владеть	ПК-7: Знать, уметь, владеть	ПК-13: Знать, уметь, владеть
минимальный	Слабо ориентируется в терминологии и содержании	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала
	Не выделяет основные идеи	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами
	Допускает грубые ошибки	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход

базовый	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал
	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике
	Может изложить основные рабочие категории	Знает основные отличия концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	Ориентируется в терминологии содержания	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	Выделяет основные идеи, но не видит их в развитии	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области
	Допускает ошибки при выделении рабочей области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Может дать критический анализ современным проблемам в заданной области анализа

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Способен выделить основные идеи текста, работает с критической литературой	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала
	не умеет	не выделяет основные идеи	Способен показать основную идею в развитии	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами
	не знает	допускает грубые ошибки	Знает основные рабочие категории, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход
базовый	не владеет	плохо ориентируется в терминологии и содержании	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал
	не умеет	выделяет основные идеи, но не видит проблем	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике
	не знает	допускает много ошибок	Может изложить основные рабочие категории	Знает основные отличия концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	не владеет	ориентируется в терминологии и содержании	В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	не умеет	выделяет основные идеи, но не видит их в развитии	Может понять практическое назначение основной идеи, но затрудняется выявить ее основания	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области
	не знает	допускает ошибки при выделении рабочей области анализа	Способен изложить основное содержание современных научных идей в рабочей области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Может дать критический анализ современным проблемам в заданной области анализа

3. Структура и содержание дисциплины

Общая трудоемкость (объем) дисциплины (модуля) составляет 7 зачетных единицы (ЗЕ*), 252 академических часа.

Объем дисциплины «Блокчейн» по видам учебных занятий в академических часах)

Объём дисциплины	Всего часов
	Очная форма обучения
Общая трудоёмкость дисциплины	252
Контактная работа обучающихся с преподавателем (по видам аудиторных учебных занятий) – всего:	98
в том числе:	
лекции	42
практические занятия	
лабораторные занятия	56
Самостоятельная работа (СРС), всего:	154
В том числе	
Контрольная работа	
Вид промежуточной аттестации (зачет/экзамен)	Экзамен (7,8)

3.1. Структура дисциплины

Очное обучение

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Занятия в активной и интерактивной форме, час.	Формируемые компетенции
			Лекции	Лаборат.	Самост. работа			
1	Основы блокчейна	7	8	12	32	Защита лабораторных работ	20/10	ОПК-5 ПК-7 ПК-14
2	Криптографические основы блокчейна	7	12	14	38	Защита лабораторных работ	26/14	ОПК-5 ПК-7 ПК-14
3	Умные контракты	8	12	16	48	Защита лабораторных работ	28/14	ОПК-5 ПК-7 ПК-14
4	Приватные блокчейны	8	10	14	36	Защита лабораторных работ	24/12	ОПК-5 ПК-7 ПК-14
	ИТОГО		42	56	154		98/50	

3.2. Содержание разделов дисциплины

4.2.1. Основы блокчейна

Блокчейн: определение, свойства и примеры индустриального применения. Технология блокчейн: история, алгоритмы, принцип работы.

Блокчейн криптовалют: кошельки, транзакции. Свойства различных криптовалют. Инфраструктура функционирования криптовалюты и поддерживающие платформы. Биткоин и альткоины. Типы токенов. Покупка, использование и хранение криптовалют. Пиринговые платёжные системы. Особенности платежей с использованием криптовалют. Безопасность транзакций и крипто-кошельков. Примеры программных продуктов и приложений, использующих блокчейн-технологии

4.2.2. Криптографические основы блокчейна

Криптография с открытым ключом, RSA. ElGamal. Эллиптические кривые. Инфраструктура криптографии с открытым ключом. Доказательства с нулевым разглашением. Схемы разделения секрета.

4.2.3. Умные контракты

Объекты контрактов, особенности, принципы работы и среда применения. Примеры проектов, использующих технологию смарт-контрактов. Публичное размещение криптовалюты (ICO - Initial Coin Offering).

Блокчейн Этериум и умные контракты в нем. Лайтнинг технология.

4.2.4. Приватные блокчейны

Византийский устойчивые алгоритмы консенсуса. FLP-невозможность. Типы сетей и примеры алгоритмов консенсуса в них. Приватные блокчейны. доказательства с нулевым разглашением и приватные умные контракты. Разработка приватных блокчейнов: особенности, технологии, практика.

3.3.Семинарские, практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тематика лабораторных занятий	Форма проведения	Формируемые компетенции
1	1	Криптографические хэш-функции.	Лабораторная работа	ОПК-5 ПК-7 ПК-14
2	1	Хэш-указатели и структура данных.	Лабораторная работа	ОПК-5 ПК-7 ПК-14
3	1	Организация хранения криптовалюты	Лабораторная работа	ОПК-5 ПК-7 ПК-14
4	1	Программные продукты блокчейн	Лабораторная работа	ОПК-5 ПК-7 ПК-14

3	2	Схема разделения секрета	Лабораторная работа	ОПК-5 ПК-7 ПК-14
2	2	Доказательство с нулевым разглашением	Лабораторная работа	ОПК-5 ПК-7 ПК-14
5	2	Блокчейн инфраструктура	Лабораторная работа	ОПК-5 ПК-7 ПК-13
6	3	Интеграция блокчейн с серверными компонентами.	Лабораторная работа	ОПК-5 ПК-7 ПК-13
7	3	Блокчейн биткойна	Лабораторная работа	ОПК-5 ПК-7 ПК-13
8	3	Изучение возможностей разработки приложений на платформе Эфириум	Лабораторная работа	ОПК-5 ПК-7 ПК-13
9	3	Блокчейн Этериум	Лабораторная работа	ОПК-5 ПК-7 ПК-13
10	3	Создание смарт-контракта на платформе Эфириум	Лабораторная работа	ОПК-5 ПК-7 ПК-13
11	3	Публичное размещение криптовалюты	Лабораторная работа	ОПК-5 ПК-7 ПК-13
12	3	Организация доступа к смарт-контракту.	Лабораторная работа	ОПК-5 ПК-7 ПК-13
13	4	Византийский устойчивые алгоритмы консенсуса	Лабораторная работа	ОПК-5 ПК-7 ПК-13
14	4	Разработка приватных блокчейнов	Лабораторная работа	ОПК-5 ПК-7 ПК-13

4. Учебно-методическое обеспечение самостоятельной работы студентов и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

4.1.Текущий контроль

Текущий контроль производится путем защиты лабораторных работ и тестирования.

В конце семестра проводится тестирование по всем разделам дисциплины. Сами тесты представлены в Системе управления курсами РГГМУ (<http://moodle.rshu.ru>)

Критерии оценивания лабораторных работ.

- оценка «зачтено»: работа полностью выполнена. Даны полные ответы на

вопросы по теме работы;

- оценка «не зачтено»: работа не выполнена или при защите студент не может ясно и четко ответить на поставленные вопросы.

4.2. Методические указания по организации самостоятельной работы

Самостоятельная работа связана с изучением и конспектированием отдельных вопросов лекционного материала, выделенного преподавателем. Для успешного выполнения самостоятельной работы необходимо:

- в соответствии с заданной темой проработать соответствующий лекционный материал;
- прочитать литературу из рекомендованного списка;
- при необходимости осуществить поиск нужной информации в сети.

Контроль выполнения самостоятельной работы обучающегося осуществляется собеседованием по определению понимания изученного материала.

Контроль исполнения самостоятельных работ осуществляется преподавателем с участием студентов в форме обсуждения выполненных заданий и работ.

5.3. Промежуточный контроль: экзамен

Перечень вопросов для экзамена:

1. Отличительные свойства блокчейн технологии.
2. Предпосылки возникновения и развития блокчейн технологии.
3. Основные государственные положения, регулирующие сферу блокчейн.
4. Существующие направления в регулировании.
5. Перспективы развития распределенных реестров.
6. Влияние квантовых технологий.
7. Классификации токенов, их особенности.
8. Модели построения бизнеса для блокчейн-проектов с использованием токенов.
9. Основополагающие вопросы децентрализации. Их обоснование.
10. Открытый код. Понятие, особенности доступа, правовые аспекты.
11. Классификация крипто-кошельков.
12. Обеспечение безопасного и хранения криптовалюты.
13. Особенности криптовалютного оборота: платежные сервисы, комиссии, торги на бирже.
14. Информационные ресурсы для анализа технологических и торговых показателей в сфере блокчейн и криптовалют.
15. Существующие инфраструктурные консорциумы для блокчейн.
16. Основные роли блокчейн-пользователей. Мотивация агентов.
17. Консенсус. Правила, история, ценность. Виды консенсусов.
18. Майнинг. Технические особенности.
19. Коммерческие блокчейн-платформы.

20. Биткоин-транзакции. Понятие. Технология работы: от записи до валидации блока.
21. Ограничения биткоина.
22. Смарт-контракты как основа автоматизации.
23. Практика применения смарт-контрактов с использованием интернета вещей.
24. Шаблон проектирования data access object (DAO). Определение, особенности функционирования, стимулы поддержания и развития DAO пользователями.
25. Смарт-контракты в архитектуре DAO.
26. ICO. Определение, элементы, преимущества и недостатки.
27. Экосистема Эфириум. Отличительные особенности построения.
28. Экосистема Этериум. Отличительные особенности построения.
29. Алгоритмы консенсуса.
30. Архитектура смарт-контрактов ICO. Сильные и слабые стороны.
31. Угроза атак на блокчейн.
32. Стратегии майнинга.

Образцы билетов к экзамену

РГГМУ

Кафедра информационных технологий и систем безопасности

Дисциплина БЛОКЧЕЙН

Билет №1

1. Отличительные свойства блокчейн технологии.

2. Майнинг. Технические особенности.

Заведующий кафедрой _____ / _____ /

Оценка «**отлично**» ставится студенту, ответ которого содержит:

- глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;
- знание концептуально-понятийного аппарата всего курса; а также свидетельствует о способности:
 - самостоятельно критически оценивать основные положения курса;
 - увязывать теорию с практикой.

Оценка «отлично» не ставится в случаях систематических пропусков студентом семинарских и лекционных занятий по неуважительным причинам, а также неправильных ответов на дополнительные вопросы преподавателя.

Оценка «**хорошо**» ставится студенту, ответ которого свидетельствует о полном знании материала по программе, а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

Оценка «хорошо» не ставится в случаях пропусков студентом семинарских и лекционных занятий по неуважительным причинам.

Оценка «**удовлетворительно**» ставится студенту, ответ которого содержит:

- поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии курса;
- стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

Оценка «**неудовлетворительно**» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Генкин А., Михеев А. Блокчейн: Как это работает и что ждет нас завтра. М.: Альпина Паблишер, 2018. – 592 с.: ISBN 978-5-9614-6558-7. Режим доступа: <http://znanium.com/catalog/product/1002003>.
2. Блокчейн в системе управления знанием: монография / М.А. Сажина, С.В. Костин. М.: ИД «ФОРУМ»: ИНФРА-М, 2020. – 90 с. Текст: электронный. URL: <http://znanium.com/catalog/product/1047262>.
3. Гаврилов Л. П. Инновационные технологии в коммерции и бизнесе. Учебник для бакалавров. М.: Юрайт, 2019 – 372 с. ISBN: 978-5-9916-2452-7. Режим доступа: <https://biblio-online.ru/book/innovacionnye-tehnologii-v-kommercii-i-biznese-425884>.

б) дополнительная литература:

1. Апробация и перспективы применения технологии блокчейн на выборах за рубежом и в России / Журнал политических исследований, 2018, № 3. Режим доступа: <http://znanium.com/catalog/product/1005721>.
2. Тарасов Д., Попов А. От золота до биткойна. М.: Альпина Паблишер, 2018. – 98 с. ISBN 978-5-9614-6614-0. Режим доступа: <http://znanium.com/catalog/product/1002838>.

в) программное обеспечение и Интернет-ресурсы:

Программное обеспечение:

- windows 7
- office 2007
- dr Web
- MySQL GNU General Public License
- PHP My Admin GNU General Public License

Интернет-ресурсы

- <https://tagline.ru/database-management-systems-rating> - рейтинг сервисов и технологий

Информационно-справочные системы:

- <https://biblio-online.ru> – ЭБС Юрайт
- <http://znanium.com> – ЭБС Знаниум
- <http://www.prospektnauki.ru> – ЭБС Проспект науки
- <http://elib.rshu.ru> ЭБС ГидроМетеоОнлайн
- <https://нэб.рф> - Национальная электронная библиотека

Профессиональные базы данных

- База данных Web of Science
- База данных Scopus
- Электронно-библиотечная система elibrary

7. Методические указания для обучающихся по освоению дисциплины

Важнейшая задача самостоятельной работы студентов является обучение навыкам работы с технической литературой и программными пакетами, которые необходимы для изучения данной дисциплины. Самостоятельная работа проводится для того, чтобы студент умел самостоятельно изучать, анализировать, перерабатывать и излагать изученный материал. К основным задачам самостоятельной работы студентов следует отнести:

1) продолжение изучения дисциплины во внеаудиторное время в соответствии с программой;

2) углубленной изучение во внеаудиторное время отдельных технических вопросов, к которым студент проявляет повышенный интерес, или по заданию преподавателя;

3) развитие у студентов интереса к вопросам проектирования баз данных, которые могут возникать в их дальнейшей профессиональной деятельности.

В ходе проведения самостоятельной работы студент по рекомендации преподавателя изучает издания и статьи по дисциплине, конспектирует их, сопоставляет дискуссионные точки зрения, анализирует их, выдвигает и обосновывает свою точку зрения по обсуждаемой проблематике.

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Введение в анализ данных	Лекция, лабораторное занятие Мультимедийные технологии	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007

		dr Web
Статистический анализ данных	Лекция, лабораторное занятие Мультимедийные технологии	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web MySQL GNU PHP My Admin GNU
Интеллектуальный анализ данных		https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web MySQL GNU PHP My Admin GNU

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитория для проведения лабораторных занятий – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования, компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации и техническими средствами обучения для выполнения лабораторных работ.

Учебная аудитория для курсового проектирования (выполнения курсовых работ) - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Учебная аудитория для текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации