Министерство науки и высшего образования РФ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники».

УТВЕРЖДАЮ

Проректор по УР

_____ И.Г. Игнатова

_____2019

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА В СЕНСОРНЫХ СИСТЕМАХ

Программа повышения квалификации разработана в Центре НТИ «Сенсорика»

Москва — 2019

1. Цель реализации программы

Цель программы – сформировать у слушателей технические знания работы систем распределенного реестра и методов и технологий на основе которых построены системы распределенного реестра, сформировать навыки практической работы с наиболее распространенными системами распределенного реестра.

2. Требования к результатам обучения

Формируемая профессиональная компетенция – способен самостоятельно разбираться в принципах и технических особенностях работы технологии распределенного реестра, администрировать и разрабатывать приложений для систем распределенного реестра.

В результате освоения данной программы слушатель должен:

***Знать**:*

- термины и понятия используемые в технологии;
- возможности и ограничения технологии;
- методы достижения консенсуса в распределенных системах;
- основные криптографические методы и примитивы используемые в технологии;
- понятие смарт-контрактов и их применение;
- направления развития технологии для снятия существующих ограничений;
- стандартизацию в области технологии: отраслевую, государственную и международную;
- основные угрозы и методы обеспечение безопасности технологи;
- основные сценарии применения технологии;

Уметь:

- мотивированно выбирать варианты применения технологии;
- устанавливать и настраивать программное обеспечение для работы серверных и клиентских компонент технологии;

- разрабатывать, тестировать и запускать на исполнение в сети распределенного реестра смарт-контракты;
- использовать базовые сервисы сети распределенного реестра;
- интерпретировать метаданные смарт-контрактов и организовывать взаимодействие между смарт-контрактами.

3. Содержание программы

Учебный план

программы повышения квалификации

«Применение технологии распределенного реестра в сенсорных системах»

Категория слушателей – студенты старших курсов ВУЗ, специалисты с высшим техническим образованием

Срок обучения – 72 часа

Форма обучения – очная

№	Наименование разделов	Всего, час	В том числе	
			Лекции	Практические и лабораторные занятия
1	Введение в технологию распределенного реестра	2	2	
2	Обзор технологии распределённого реестра. Рассмотрение работы распределённого реестра на примере Etherium	16	4	12
3	Базовые криптографические компоненты построения технологии распределённого реестра	14	14	
4	Введение в смарт-контраткты	16	4	12
5	Ограничения технологии распределенного реестра	4	4	
6	Стандартизация в области распределённого реестра	4	4	
7	Вопросы безопасности технологии	6	6	

	распределенного реестра			
8	Рассмотрение примеров применения технологии распределенного реестра для конкретных задач	8	4	4
9	Консультация	2		
	Всего	72	42	28
Итоговая аттестация		Итоговый тест		

Учебно-тематический план
программы повышения квалификации
«Применение технологии распределенного реестра в сенсорных системах»

№	Наименование разделов	Всего, час	В том числе	
			Лекции	Практические и лабораторные занятия
1	**Введение в технологию распределенного реестра**	**2**	**2**	
1.1	История создания технологии распределенного реестра	1	1	
1.2	Определение понятия, возможности и классификация технологии распределённого реестра	1	1	
2	**Обзор технологии распределённого реестра. Рассмотрение работы распределённого реестра на примере Etherium**	**16**	**4**	**12**
2.1	Общее описание работы Etherium: структура блоков Etherium, достижение консенсуса, распределенный протокол взаимодействия, основные возможности	6	2	4
2.2	Структура и принцип работы серверного узла Etherium. Сеть Etherium	5	1	4
2.3	Порядок работы клиентской компоненты. Хранение информации о реестре. Протокол доступа	5	1	4
3	**Базовые криптографические компоненты**	**14**	**14**	

	построения технологии распределённого реестра			
3.1	Функция хеширования и дерево Меркеля	2	2	
3.2	Электронно-цифровая подпись и ее разновидности: слепая подпись, кольцевая подпись, подписи Шнорра	2	2	
3.3	Интерактивные протоколы с нулевым разглашением	2	2	
3.4	Неинтерактивные протоколы с нулевым разглашением	2	6	
3.5	Методы достижение консенсуса	2	2	
4	**Введение в смарт-контракты**	**16**	**4**	**12**
4.1	Понятие смарт-контракта. Смарт-контракты на примере Ethereum	1	1	
4.2	Ведение в возможности языка Solidity	5	1	4
4.3	Примеры возможных бизнес-логик и применений смарт-контрактов	5	1	4
4.4	Примеры реализации смарт-контрактов	5	1	4
5	**Ограничения технологии распределенного реестра**	**4**	**4**	
5.1	Основные ограничения связанные с числом обрабатываемых транзакция и прочие ограничения	2	2	
5.2	Ограничения по достижению консенсуса, проблемы с PoW	1	2	
5.3	Основные механизмы преодоления существующих ограничений предлагаемые для проекта Bitcoin	2	2	
6	**Стандартизация в области распределённого реестра**	**4**	**4**	
6.1	Стандартизация базовых компонент, стандарты на криптографические алгоритмы и коммуникационные протоколы	2	2	
6.2	Стандартизация технологии в США, в России, в Республике Беларусь, ISO. Отраслевая	2	2	

	стандартизация ITEF, в проектах Bitcoin, Ethereum и Hyperledger			
7	**Вопросы безопасности технологии распределенного реестра**	**6**	**6**	
7.1	Общая постановка вопроса обеспечения безопасности технологии, угрозы технологии	1	1	
7.2	Анонимные распределённые реестры на примере проекта Zcash и Monero	3	3	
7.3	Реестры с безопасными распределенными вычислениями на примере проекта Enigma	2	2	
8	**Рассмотрение примеров применения технологии распределенного реестра для конкретных задач**	**8**	**4**	**4**
8.1	Система распределенного сбора данных от различных датчиков	1	1	
8.2	Приобретение билетов и программа лояльности на основе распределенного реестра в авиакомпании	1	1	
8.3	Применение для технологий электронной идентификации и аутентификации	1	1	
8.4	Распределенные реестры с управлением доступа на примере Hyperledger	5	1	4
9	Консультации	2		
	Всего	72	42	28
Итоговая аттестация:		Итоговый тест		

Учебная программа
повышения квалификации
«Применение технологии распределенного реестра в сенсорных системах»

Модуль 1. Введение в технологию распределенного реестра (2 часа)

Тема 1.1. Определение основных понятий в распределённом реестре.

Тема 1.2. Определение понятия, возможности и классификация технологии распределённого реестра.

Модуль 2. Обзор технологии распределённого реестра. Рассмотрение работы распределённого реестра на примере Etherium (16 часаов)

Тема 2.1. Общее описание работы Etherium: структура блоков Etherium, достижение консенсуса, распределенный протокол взаимодействия, основные возможности.

Тема 2.2. Структура и принцип работы серверного узла Etherium. Сеть Etherium.

Тема 2.3. Порядок работы клиентской компоненты. Хранение информации о реестре. Протокол доступа.

Модуль 3. Базовые криптографические компоненты построения технологии распределённого реестра (14 часов)

Тема 3.1. Функция хеширования и дерево Меркеля.

Тема 3.2. Электронно-цифровая подпись и ее разновидности: слепая подпись, кольцевая подпись, подписи Шнорра.

Тема 3.3. Интерактивные протоколы с нулевым разглашением.

Тема 3.4. Неинтерактивные протоколы с нулевым разглашением.

Тема 3.5. Методы достижение консенсуса (PoS, PoW и другие).

Модуль 4. Введение в смарт-контракты (16 часов)

Тема 4.1. Понятие смарт-контракта. Смарт-контракты на примере Ethereum.

Тема 4.2. Ведение в возможности языка Solidity.

Тема 4.3. Примеры возможных бизнес-логик и применений смарт-контрактов.

Тема 4.4. Примеры реализации смарт-контрактов.

Модуль 5. Ограничения технологии распределенного реестра (4 часа)

Тема 5.1. Основные ограничения связанные с числом обрабатываемых транзакция и прочие ограничения.

Тема 5.2. Ограничения по достижению консенсуса, проблемы с PoW.

Тема 5.3. Основные механизмы преодоления существующих ограничений предлагаемые для проекта Bitcoin.

Модуль 6. Стандартизация в области распределённого реестра (2 часа)

Тема 6.1. Стандартизация базовых компонент, стандарты на криптографические алгоритмы и коммуникационные протоколы.

Тема 6.2. Стандартизация технологии в США, в России, в Республике Беларусь, ISO. Отраслевая стандартизация ITEF, в проектах Bitcoin, Ethereum и Hyperledger.

Модуль 7. Вопросы безопасности технологии распределенного реестра (4 часа)

Тема 7.1. Общая постановка вопроса обеспечения безопасности технологии, угрозы технологии.

Тема 7.2. Анонимные распределённые реестры на примере проекта Zcash и Monero.

Тема 7.3. Реестры с безопасными распределенными вычислениями на примере проекта Enigma.

Модуль 8. Рассмотрение примеров применения технологии распределенного реестра для конкретных задач (8 часов)

Тема 8.1. Система распределенного сбора данных от различных датчиков.

Тема 8.2. Приобретение билетов и программа лояльности на основе распределенного реестра в авиакомпании.

Тема 8.3. Применение для технологий электронной идентификации и аутентификации.

Тема 8.4. Распределенные реестры с управлением доступа на примере Hyperledger.

Перечень практических занятий

Практические занятия не предусмотрены.

Перечень лабораторных работ

Номер темы	Наименование практического занятия	Кол-во часов
2.1	Установка и настройка тестовой сети Ethereum	4
2.2	Установка и настройка клиента сети Ethereum	4
2.3	Работа с Mist Ethereum	4
4.2	Интегрированная среда разработки Mix	4
4.3	Solidity. Разработка и запуск смарт-контрактов в сети Ethereum	4
4.4	Отладка и тестирование контрактов в сети Ethereum	4
8.4	Разработка контракта. Метаданные контракта. Взаимодействие между контрактами	4

4. Материально-технические условия реализации программы

Наименование специализированных аудиторий кабинетов,	Вид занятия	Наименование оборудования, программного обеспечения

лабораторий		
Лабораторный компьютерный класс	Лабораторные работы	Персональный компьютер с установленным средством визуализации VirtualBox
Лекционный класс	Лекции	Персональный компьютер с установленным программным обеспечением для показа презентаций в формате Open Document Format Presentation, проектор, проекционный экран

5. Учебно-методическое обеспечение программы

Для успешного освоения программы слушатели должны иметь доступ к сети Интернет и следующей литературе:

1. В.Г. Олифер, Н.А. Олифер. Безопасность компьютерных сетей. – М.: Горячая линия – Телеком, 2019;
2. Введение в криптографию / Под общей ред. В.В. Ященко. – СПб.: Питер, 2001;
3. Шаньгин В.Ф. Информационная безопасность. - М.: ДМК Пресс, 2014;
4. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. -Спб.: БХВ-Питербург, 2009;
5. Прасти Н. Блокчейн. Разработка приложений: Пер. с англ. — СПб.: БХВ-Петербург, 2018.

6. Оценка качества освоения программы

Оценка качества усвоения программы осуществляется путем устного тестирования и по результатам выполнения слушателями лабораторных работ. Критериями оценки является наличие у слушателей ниже приведенных теоретических знаний и демонстрации им в процессе выполнения лабораторных работ ниже приведенных практических навыков.

После освоения программы слушатель должен продемонстрировать следующие знания:

- профессиональной терминологии в области технологии распределенного реестра;
- возможностей, преимуществ и недостатков технологии распределенного реестра;

- работы базовых вариантов технологии распределенного реестра;
- базовых примитивов лежащих в основе технологии распределенного реестра (дерево Меркеля, методы достижение консенсуса, слепая подпись, кольцевая подпись, подписи Шнорра, протоколы с нулевым разглашением);
- назначение, возможности и принципы использования смарт-контрактов;
- основ синтаксиса и семантики языка Solidity;
- основных методов достижения консенсуса;
- стандартов в области технологии распределенного реестра;
- угроз для систем распределенного реестра и методов предотвращения этих угроз;
- основных вариантов применения технологии распределенного реестра.

После освоения программы слушатель должен уметь:

- установить и настроить тестовую сеть Ethereum;
- установить и настроить клиентское приложение сети Ethereum;
- работать с клиентским приложением Mist Ethereum;
- работать в интегрированной среде разработки Mix;
- разрабатывать смарт-контракты на языке Solidity;
- разрабатывать, отлаживать и запускать смарт—контракты в тестовой сети Ethereum;
- использовать базовые сервисы сети Ethereum: Whisper, Swarm, Alarm Clock, Computation Market, BTCRelay, RANDO;
- использовать метаданные контракта для его корректного настройки и исполнения.

7. Составители программы

Доцент кафедры ТКС, к.т.н. _____ / А.В. Шарамок /