**Концепция вариативной профессиональной компетенции**

*«Способен создавать и исследовать решения различного назначения на базе технологии блокчейн»*

для направлений магистратуры ЮФУ, относящихся к области 06 (Связь, информационные и коммуникационные технологии) и сфере профессиональной деятельности по проектированию и разработке программного обеспечения

1) *общее описание концепции вариативной ПК, включая обоснование актуальности компетенции и её востребованности у выпускников направления подготовки и/или специальности, для которой предлагается данная компетенция*

Системы распределенного реестра стали занимать отдельную нишу в современном стеке информационных технологий. Платформы, базирующиеся на блокчейн технологиях, начиная от криптовалютных систем, заканчивая различными сервисами с контролем выполнения обязательств, приобретают свою популярность за счет механизмов обеспечения целостности, которыми они обладают. Технология стала завоевывать доверие на рынке информационных решений. Однако, как и у любой технологии у систем распределенных реестров есть свои особенности, которые требуют к себе внимания. Сегодня основными проблемами блокчейна являются необходимость хранения большого объема данных, сложности при масштабируемости, возможные денежные риски, связанные с кражей данных, уязвимости, возможные при непрофессиональной разработке систем. В связи с этим становится актуальным вопрос контроля безопасности таких решений с целью предотвращения описанных рисков. В научном сообществе еще не так много работ по стороннему анализу, изучению и тестированию существующих платформ.

2) *область и сферы профессиональной деятельности в рамках направления подготовки / специальности, тип задач и задачи профессиональной деятельности, к решению которых будет подготовлен выпускник, освоивший данную компетенцию*

Общая характеристика профессиональной деятельности

| *Области и сферы профессиональной деятельности* | *Типы задач (виды) и задачи профессиональной деятельности* | *Объекты профессиональной деятельности*  *(или области знаний)* |
| --- | --- | --- |
| 06 Связь, информационные и коммуникационные технологии (в сфере проектирования и разработки программного обеспечения) | Проектный тип задач:  1. Разработка и реализация блокчейн-систем с использованием заданных криптографических протоколов  2. Оценка защищенности заданного блокчейн-решения | Блокчейн-системы  Программные средства  Криптографические протоколы  Безопасность криптографических протоколов |

*3) основание разработки вариативной ПК (например, профессиональный стандарт, а также обобщённые трудовые функции и трудовые функции, к выполнению которых будет подготовлен выпускник, освоивший данную компетенцию)*

Перечень профессиональных стандартов, обобщённых трудовых и трудовых функций

| Код и наименование профессионального стандарта | Код и наименование обобщённой трудовой функции | Код и наименование трудовой функции | Уровень квалифи­кации |
| --- | --- | --- | --- |
| 06.033 Специалист по защите информации в автоматизированных системах | D.7 Разработка систем защиты информации автоматизированных систем | D/01.7 Тестирование систем защиты информации автоматизированных систем | 7 |
| D/02.7 Разработка проектных решений по защите информации в автоматизированных системах | 7 |
| D/04.7 Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем | 7 |

*4) формулировка вариативной ПК и индикаторов её достижения, соотнесённых с задачами профессиональной деятельности и основаниями разработки вариативной ПК*

Вариативные профессиональные компетенции и индикаторы их достижения

| Код и наименование профессиональной компетенции | Код и наименование индикатора достижения профессиональной компетенции | Задачи профессиональной деятельности | Основание |
| --- | --- | --- | --- |
| Проектный тип задач профессиональной деятельности | | | |
| ВПК-1. Способен создавать и исследовать решения различного назначения на базе технологии блокчейн | ВПК-1.1. Выбирает необходимый криптографический протокол и выполняет его программную реализацию | Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы | ПС 06.033 |
| ВПК-1.2. Выбирает механизм консенсуса, разрабатывает и реализует архитектуру безопасного блокчейн решения | Составляет комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе | ПС 06.033 |
| ВПК-1.3. Формулирует перечень возможных угроз безопасности, осуществляет проверку основных сценариев тестирования блокчейн-решений | Выявление угроз безопасности информации в автоматизированных системах | ПС 06.033 |

*5) трудоёмкость и структура модуля ББТ, предназначенного для формирования компетенции; при этом модуль ББТ должен предусматривать выполнение проекта или проведение практико-ориентированного экзамена, направленных на комплексную оценку сформированности компетенции*

**5.1. Содержание модуля «Модуль по безопасности блокчейн технологий» (ББТ):**

* дисциплина «Криптографические протоколы для современных блокчейн систем» – 3 семестр, 8 ЗЕТ, 36 часов лекций, 36 часов практик, практико-ориентированный проект, практикоориентированный экзамен, индикаторы ВПК-1.1, ВПК-1.2.
* дисциплина «Безопасность решений на основе использования блокчейн-технологий» - 3 семестр, 5 ЗЕТ, 18 часов лекций, 18 часов практик, индивидуальный проект, онлайн курсы, диф.зачет, индикатор ВПК-1.3.

**5.2. Содержание дисциплины «Криптографические протоколы для современных блокчейн систем»:**

***Модуль 1.***

Темы лекционных занятий:

*Тема 1. Криптографические методы для блокчейн-систем. Асимметричная криптография. Выработка ключей для асимметричных систем. ЭЦП, контроль целостности, дерево Меркля.*

*Тема 2. Протоколы консенсуса. Доказательство работы, доказательство доли, задача о византийских генералах и другие.*

*Тема 3. Протоколы идентификации-аутентификации. Парольные схемы. Схемы типа «запрос-ответ». Протокол рукопожатия.*

*Тема 4. Протоколы распределенного хранения ключей. Китайская теорема об остатках. Схема Блекли. Схема Шамира.*

Темы практических (семинарских) занятий

Тема 1. Алгоритм RSA.

Тема 2. Поиск nonce для протокола консенсуса Доказательство работы.

Тема 3. Построение схемы аутентификации для заданной блокчейн-системы.

Тема 4. Распределение ключа по заданному протоколу.

***Модуль 2.***

Темы лекционных занятий:

*Тема 5. Протоколы с нулевым разглашением знания.*

*Тема 6. Протоколы электронного голосования. Протоколы тайного электронного голосования.*

*Тема 7. Протоколы распределения и обмена ключами*

*Тема 8. Оракулы в области блокчейн-технологий*

Темы практических (семинарских) занятий

Тема 5. Основы реализации протокола с нулевым разглашением знания.

Тема 6. Основы реализации протокола электронного голосования.

Тема 7. Основы реализации протокола распределения ключа.

Тема 8. Построение схемы работы оракула для блокчейн-системы.

**Результат изучения дисциплины:**

Выполнение индивидуального задания по разработке и реализации блокчейн-системы с использованием заданных криптографических протоколов

**5.3. Содержание дисциплины «Безопасность решений на основе использования блокчейн-технологий»:**

***Модуль 1.***

Темы лекционных занятий

*Тема 1. Типы уязвимостей в блокчейн-системах.*

*Тема 2. Уязвимости современных блокчейн-платформ. На примере платформ Ethereum, Hyper Ledger, EOS, NEO.*

*Тема 3. Обзор потенциальных кибератак на криптовалюты. Стоимость проводимых атак.*

Перечень тем практических занятий

*Практическая работа №1*

*Рассмотрение кейсов по уязвимости блокчейн систем.*

*Практическая работа №2*

*Разработка схем по устранению существующих уязвимостей блокчейн систем.*

*Практическая работа №3*

*Разработка стратегии защиты от потенциальных атак.*

***Модуль 2.***

Темы лекционных занятий:

*Тема 4. Методы построения смарт-контрактов. Смарт-контракт для системы Ethereum. Язык Solidity.*

*Тема 5. Основные уязвимости смарт-контрактов Ethereum. Методы тестирования логики работы смарт-контрактов Ethereum.*

*Тема 6. Основные уязвимости клиентского приложения для работы с блокчейн-системой.*

Перечень тем практических занятий

*Практическая работа №5*

*Создание смарт-контракта на заданную тему*

*Практическая работа №6*

*Создание клиентского приложения для работы смарт-контракта*

*Практическая работа №7*

*Покрытие смарт-контракта тестами*

*Практическая работа №8*

*Покрытие клиентского приложения тестами*

**Результат изучения дисциплины:**

Выполнение индивидуального задания по проведению оценки защищенности заданного блокчейн-решения.

**Сопутствующие онлайн-курсы:**

* Онлайн-курс Асимметричная криптография и управление ключами (язык: английский) [https://www.coursera.org/learn/asymmetric-crypto/](https://vk.com/away.php?to=https%3A%2F%2Fwww.coursera.org%2Flearn%2Fasymmetric-crypto%2F&cc_key=)
* Онлайн-курс Хэш и целостность информации (язык: английский) <https://www.coursera.org/learn/cryptographic-hash-int>
* Онлайн-курс Основы и практическое применение блокчейна (язык: русский) [https://www.coursera.org/learn/blokcheyna](https://vk.com/away.php?to=https%3A%2F%2Fwww.coursera.org%2Flearn%2Fblokcheyna&cc_key=)
* Онлайн-курс Основы блокчейн (язык: английский) [https://www.coursera.org/learn/blockchain-basics](https://vk.com/away.php?to=https%3A%2F%2Fwww.coursera.org%2Flearn%2Fblockchain-basics&cc_key=)
* Онлайн-курс Смарт-контракты на Ethereum (язык: английский) [https://www.coursera.org/learn/smarter-contracts](https://vk.com/away.php?to=https%3A%2F%2Fwww.coursera.org%2Flearn%2Fsmarter-contracts&cc_key=)
* Онлайн-курс Децентрализованные приложения (язык: английский) [https://www.coursera.org/learn/decentralized-apps-on-..](https://vk.com/away.php?to=https%3A%2F%2Fwww.coursera.org%2Flearn%2Fdecentralized-apps-on-blockchain&cc_key=)
* Онлайн-курс Блокчейн платформы (язык: английский) [https://www.coursera.org/learn/blockchain-platforms](https://vk.com/away.php?to=https%3A%2F%2Fwww.coursera.org%2Flearn%2Fblockchain-platforms&cc_key=)

*6) краткая характеристика применяемых образовательных технологий, кадрового и материально-технического обеспечения.*

Наряду с традиционными образовательными технологиями, для реализации модуля ББТ могут использоваться технологии электронного обучения и дистанционные образовательные технологий в электронной информационно-образовательной среде Южного федерального университета.

Модуль ББТ может быть реализован с использованием электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ) в ЭИОС Университета, включая систему электронного обучения ИКТИБ (lms.sfedu.ru). Аудиторные занятия и другие формы контактной работы обучающихся с преподавателем могут проводиться с использованием платформ MicrosoftTeams, Cisco, Skype, Google Classroom, Zoom и др., что позволяет обеспечить онлайн и офлайн взаимодействие преподавателя с обучающимися.

Основными методами текущего контроля являются электронный учёт и контроль учебных достижений студентов (использование средств сервиса балльно-рейтинговой системы; ведение электронного журнала успеваемости, проведение электронного тестирования и применение других средств контроля с использованием системы электронного обучения).

По дисциплине «Криптографические протоколы для современных блокчейн систем» в рамках текущего контроля оценивается подготовка доклада, выступление и участие в обсуждении тем практических (семинарских) занятий, выполнение заданий на практических работах.

По дисциплине «Анализ уязвимостей решений на основе использования блокчейн-технологий» в рамках текущего контроля оценивается выполнение практических заданий.

Мероприятиями рубежного контроля являются контрольные работы (в рабочих программах дисциплин представлены банки тестовых заданий по каждому пройденному модулю дисциплин), а также практикоориентированные индивидуальные проектные задания.

По дисциплине «Криптографические протоколы для современных блокчейн систем» промежуточная аттестация запланирована в форме практикоориентированного экзамена, который предполагает ответ на вопрос по терминологии в области тестирования (20 баллов) и собеседование по практическому индивидуальному заданию (20 баллов), работу над которым магистрант выполнял в течение семестра. Формой промежуточной аттестации по дисциплине «Анализ уязвимостей решений на основе использования блокчейн-технологий» является дифференцированный зачет.

Самостоятельная работа магистрантов предполагает изучение теоретического материала (проработку конспектов лекций, работу с учебной литературой и информационно-образовательными ресурсами), подготовку к практическим занятиям, выполнение практических заданий, написание отчета по выполненному проекту *а также выбор индивидуальной траектории в виде вариативного трека, обеспечиваемого самостоятельным дистанционным освоением онлайн-курсов. Выбор рекомендуется проводить исходя из предпочитаемого в профессиональной деятельности стека технологий программирования.*

Все обучающиеся обеспечены неограниченным доступом к электронной информационно-образовательной среде Южного федерального университета, электронным библиотечным системам, профессиональным базам данных и информационным справочным системам. Все обучающиеся имеют доступ в помещения для самостоятельной работы, оснащённые компьютерной техникой, подключённой к сети «Интернет».

Материально-техническое обеспечение (включая используемые учебные аудитории, перечни оборудования, технических средств обучения, лицензионного и свободно распространяемого программного обеспечения) и учебно-методическое обеспечение образовательной программы представлены в рабочих программам дисциплин.

Реализация модуля ББТ планируется обеспечить педагогическими работниками Южного федерального университета, квалификация которых удовлетворяет квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах, а также привлечь работников из числа руководителей и сотрудников организаций, деятельность которых непосредственно связана с тематикой ББТ. Заинтересованность в реализации модуля (в первую очередь в формате открытых лекций, мастер-классов, кейсов для выполнения практических занятий) уже проявили несколько профильных компаний, в частности компании i-link и Росатом.

*7) язык реализации модуля ББТ, формирующего компетенцию:*

русский

Инициативная группа:

*Ищукова Е.А..* доц. каф. БИТ, к.т.н., доцент, менеджер компетенции «Разработка решений с использованием блокчейн технологий» в движении WorldSkills

*Салманов В.Д..* программист ИКТИБ, призер Чемпионата Мира по стандартам WorldSkills Kazan-2019 в компетенции «Разработка решений с использованием блокчейн технологий», эксперт WorldSkills в компетенции «Разработка решений с использованием блокчейн технологий»

*Романенко К.С.,* лаборант каф. САиТ ИКТИБ, эксперт WorldSkills в компетенции «Разработка решений с использованием блокчейн технологий»

*15.12.2020*