

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Галунин Сергей Александрович
Должность: проректор по учебной работе
Дата подписания: 27.07.2022 11:31:08
Уникальный программный ключ:
08ef34338325bdb0ac5a47baa5472ce36cc3fc3b

Приложение к ОПОП
«Безопасность и этика искус-
ственного интеллекта»



СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
**«Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)»**

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«ТЕХНОЛОГИИ И ПРОТОКОЛЫ КРИПТОВАЛЮТ»

для подготовки магистров

по направлению

09.04.01 «Информатика и вычислительная техника»

по программе

«Безопасность и этика искусственного интеллекта»

Санкт-Петербург

2021

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

д. ф.-м. н Широков И.В.

Рабочая программа рассмотрена и одобрена на заседании кафедры ВТ
02.09.2021, протокол № 6

Рабочая программа рассмотрена и одобрена учебно-методической комиссией
ФКТИ, 16.09.2021, протокол № 6

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	ИС
Общая трудоемкость (ЗЕТ)	2
Курс	2
Семестр	3
Виды занятий	
Лекции (академ. часов)	8
Практические занятия (академ. часов)	9
Все контактные часы (академ. часов)	17
Самостоятельная работа, включая часы на контроль (академ. часов)	55
Всего (академ. часов)	72
Вид промежуточной аттестации	
Дифф. зачет (курс)	2

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«ТЕХНОЛОГИИ И ПРОТОКОЛЫ КРИПТОВАЛЮТ»

Целью изучения дисциплины «Технологии и протоколы криптовалют» является повышение квалификации и совершенствование компетенций по ключевым вопросам теории и практики создания и функционирования криптовалют и технологии блокчейн, их применение в области защиты информации.

SUBJECT SUMMARY

«CRYPTOCURRENCY TECHNOLOGIES AND PROTOCOLS»

The purpose of studying the discipline "Technologies and Protocols of Cryptocurrency" is to improve skills and improve competencies on key issues of theory and practice of the creation and functioning of cryptocurrencies and blockchain technology, their application in the field of information security.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Целью изучения дисциплины «Технологии и протоколы криптовалют» является повышение квалификации и совершенствование компетенций по ключевым вопросам теории и практики создания и функционирования криптовалют и технологии блокчейн, их применение в области защиты информации.

2. Задачи дисциплины:

ознакомить будущих специалистов с технологией блокчейна и протоколами криптовалют;

показать необходимость усвоения знаний о технологиях блокчейна и протоколов криптовалют;

научить применять технологии блокчейна и протоколы криптовалют при построении комплексных систем защиты информации.

3. Знания общих принципов функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети.

4. Умение определять механизм изменения и модификации базовой конфигурации.

5. Владеть навыками настройки параметров управления безопасностью операционных систем сетевых устройств.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Производственная практика (технологическая (проектно-технологическая) практика)»

и обеспечивает подготовку выпускной квалификационной работы.

3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	Наименование компетенции/индикатора компетенции
ПК-30	Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях
<i>ПК-30.1</i>	<i>Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях</i>

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	СР, ач
1	Система "Биткойн". Протокол "электронной наличности".	1	1	8
2	Протокол Hashcash. Дерево Меркля. Блокчейн. Алгоритм цифровой подписи ECDSA.	2	2	13
3	Адресация в системе «Биткойн». Структура блока транзакций. Майнинг. Проблема масштабируемости биткойна.	2	2	14
4	Программное обеспечение сети «Биткойн». «Умные контракты». Системы Ripple и Ethereum.	2	2	10
5	«Цветные монеты». Основные блокчейн-платформы. Правовой режим криптовалют.	1	2	10
	Итого, ач	8	9	55
	Из них ач на контроль	0	0	0
	Общая трудоемкость освоения, ач/зе	72/2		

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Система "Биткойн". Протокол "электронной наличности".	Система "Биткойн". Протокол "электронной наличности".
2	Протокол Hashcash. Дерево Меркля. Блокчейн. Алгоритм цифровой подписи ECDSA.	Протокол Hashcash. Дерево Меркля. Блокчейн. Алгоритм цифровой подписи ECDSA.
3	Адресация в системе «Биткойн». Структура блока транзакций. Майнинг. Проблема масштабируемости биткойна.	Адресация в системе «Биткойн». Структура блока транзакций. Майнинг. Проблема масштабируемости биткойна.
4	Программное обеспечение сети «Биткойн». «Умные контракты». Системы Ripple и Ethereum.	Программное обеспечение сети «Биткойн». «Умные контракты». Системы Ripple и Ethereum.
5	«Цветные монеты». Основные блокчейн-платформы. Правовой режим криптовалют.	«Цветные монеты». Основные блокчейн-платформы. Правовой режим криптовалют.

4.2 Перечень лабораторных работ

Лабораторные работы не предусмотрены.

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. История создания системы «Биткойн».	0.5
2. Протоколы «электронной наличности», система доказательства выполнения работы.	0.5
3. Изучить структуру протокола Hashcash и его применение на практике.	0.5
4. Изучить структуру дерева Меркля и его применение на практике.	0.5
5. Создание структуры блокчейн. Работа с блоками.	0.5
6. Изучить алгоритм цифровой подписи ECDSA	0.5
7. Принцип работы адресации в системе «Биткойн».	0.5
8. Изучить структуру блока транзакций.	0.5
9. Изучить структуру алгоритма майнинга и применить его на практике.	1
10. Рассмотреть проблему масштабируемости биткойна. Предложить решения данной проблемы.	0.5
11. Рассмотреть программное обеспечение сети «Биткойн».	1
12. Смарт-контракты: как они работают и зачем нужны.	1
13. Изучить основные преимущества «цветных монет».	0.5
14. Рассмотреть основные блокчейн-платформы, провести их сравнение.	0.5
15. Изучить правовой режим криптовалют.	0.5
Итого	9

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

Индивидуальное домашнее задание не предусмотрено.

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа направлена на закрепление и углубление полученных теоретических и практических знаний, развитие навыков практической работы.

Текущая СРС	Примерная трудоемкость, ач
Работа с лекционным материалом, с учебной литературой	10
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	0
Самостоятельное изучение разделов дисциплины	0
Выполнение домашних заданий, домашних контрольных работ	0
Подготовка к лабораторным работам, к практическим и семинарским занятиям	20
Подготовка к контрольным работам, коллоквиумам	10
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	0
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	0
Подготовка к зачету, дифференцированному зачету, экзамену	15
ИТОГО СРС	55

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Мельников, Владимир Павлович. Информационная безопасность и защита информации [Текст] : учеб. пособие для вузов по специальности "Информац. системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова, 2012. -330, [1] с.	7
2	Гашков, Сергей Борисович. Криптографические методы защиты информации [Текст] : учеб. пособие для вузов по направлению "Прикладная математика и информатика" и "Информац. технологии" / С. Б. Гашков, Э. А. Применко, М. А. Черепнев, 2010. -297, [1] с.	5
Дополнительная литература		
1	Прохорова, Ольга Витольдовна. Информационная безопасность и защита информации [Текст] : учеб. / О. В. Прохорова, 2020. -121 с.	39

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	Что такое технология блокчейна? https://www.ibm.com/ru-ru/topics/what-is-blockchain
2	Проекты на базе блокчейн технологии https://www.tadviser.ru/index.php/Продукт:Проекты_технологии
3	Криптовалюты в реальном времени https://ru.investing.com/crypto/

5.3 Адрес сайта курса

Адрес сайта курса: <https://vec.etu.ru/moodle/course/view.php?id=8915>

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Технологии и протоколы криптовалют» формой промежуточной аттестации является зачет с оценкой.

Зачет с оценкой

Оценка	Описание
Неудовлетворительно	Курс не освоен. Студент испытывает серьезные трудности при ответе на ключевые вопросы дисциплины
Удовлетворительно	Студент в целом овладел курсом, но некоторые разделы освоены на уровне определений и формулировок теорем
Хорошо	Студент овладел курсом, но в отдельных вопросах испытывает затруднения. Умеет решать задачи
Отлично	Студент демонстрирует полное овладение курсом, способен применять полученные знания при решении конкретных задач.

Особенности допуска

Выполнение всех практических работ.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Примерные вопросы к дифф.зачету

№ п/п	Описание
1	История создания системы «Биткойн».
2	Протоколы «электронной наличности», система доказательства выполнения работы.
3	Протокол Hashcash и его применение.
4	Дерево Меркля.
5	Блокчейн. Алгоритм цифровой подписи ECDSA.
6	Адресация в системе «Биткойн».
7	Структура блока транзакций. Майнинг.
8	Проблема масштабируемости биткойна.
9	Программное обеспечение сети «Биткойн».
10	«Умные контракты».
11	Системы Ripple и Ethereum.
12	«Цветные монеты».
13	Основные блокчейн-платформы.
14	Правовой режим криптовалют.

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
1	Система "Биткойн". Протокол "электронной наличности".	
2		Практическая работа
3	Протокол Hashcash. Дерево Меркля. Блокчейн. Алгоритм цифровой подписи ECDSA.	
4		
5		
6		Практическая работа
7	Адресация в системе «Биткойн». Структура блока транзакций. Майнинг. Проблема масштабируемости биткойна.	
8		
9		
10		Практическая работа
11	Программное обеспечение сети «Биткойн». «Умные контракты». Системы Ripple и Ethereum.	
12		
13		Практическая работа

6.4 Методика текущего контроля

на лекционных занятиях

Текущий контроль включает в себя контроль посещаемости (не менее 80% занятий), по результатам которого студент получает допуск на дифференцированный зачет.

на практических (семинарских) занятиях

Текущий контроль включает в себя контроль посещаемости (не менее 80% занятий), по результатам которого студент получает допуск на дифференцированный зачет. В ходе проведения семинарских и практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методикам, описанным выше.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, IBMсовместимый компьютер Pentium или выше, проектор, экран, меловая или маркерная доска	1) Windows 7 и выше; 2) Microsoft Office 2007 и выше
Практические занятия	Компьютерный класс	ест, оборудованных персональными IBMсовместимыми компьютерами Pentium или выше в соответствии с контингентом, рабочее место преподавателя, IBMсовместимый компьютер Pentium или выше, проектор, экран, меловая или маркерная доска	1) Windows 7 и выше; 2) Microsoft Office 2007 и выше
Самостоятельная работа	Помещение для самостоятельной работы	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА