ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 01.02.2022

А. В. Голлай

РАБОЧАЯ ПРОГРАММА
практики
к ОП ВО от 01.07.2020 №084-2629

Практика Учебная практика, ознакомительная практика
для направления 10.03.01 Информационная безопасность
Уровень бакалавр **Тип программы** Бакалавриат
профиль подготовки Безопасность автоматизированных систем
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утверждённым приказом Минобрнауки от 01.12.2016 № 1515

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 31.01.2022

А. Н. Соколов

Разработчик программы,
к.физ.-мат.н., доц., доцент

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Ручай А. Н.
Пользователь: ruchaian
Дата подписания: 31.01.2022

А. Н. Ручай

Челябинск

1. Общая характеристика

Вид практики

Учебная

Способ проведения

Стационарная или выездная

Тип практики

ознакомительная

Форма проведения

Дискретно по видам практик

Цель практики

Изучение линейных рекуррентных последовательностей и практического применения их для поточного шифрования.

Задачи практики

Обучение студентов основам практического применения линейных рекуррентных соотношений, которые играют важную роль не только в алгебре, теории чисел, теории кодирования и криптографии, но и в геометрии, теории оптимизации, радарной технике, системах связи и ряде других приложений.

Краткое содержание практики

В процессе практики каждый студент выполняет индивидуальное задание, посвященное линейным рекуррентным последовательностям и практическому применению их для поточного шифрования, а также выполняет разработку программы, обеспечивающей решение поставленной задачи.

2. Компетенции обучающегося, формируемые в результате прохождения практики

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения при прохождении практики (ЗУНы)
ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать:основные методы реализации линейных рекуррентных последовательностей и поточного шифрования на их основе.
	Уметь:проводить анализ криптографической стойкости поточного шифрования на основе линейных рекуррентных последовательностей.

	Владеть:реализовывать поточное шифрование на основе линейных рекуррентных последовательностей на языках высокого уровня.
ОК-8 способностью к самоорганизации и самообразованию	Знать:базовые методы и средства самоорганизации и самообразования
	Уметь:планировать самостоятельную образовательную деятельность на основе формулирования ближайших и стратегических целей
	Владеть:навыками планирования, определения средств и целей самостоятельной деятельности
ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач	Знать:свойства основных дискретных структур: конечных полей, групп, линейных рекуррентных последовательностей.
	Уметь:решать задачи периодичности для линейных рекуррентных последовательностей.
	Владеть:аппаратом линейных рекуррентных последовательностей для поточного шифрования.

3. Место практики в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ	Перечень последующих дисциплин, видов работ
Б.1.17 Языки программирования Б.1.06.01 Алгебра и геометрия	Б.1.29 Математические основы криптологии Б.1.22 Криптографические методы защиты информации

Требования к «входным» знаниям, умениям, навыкам студента, необходимым для прохождения данной практики и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.06.01 Алгебра и геометрия	Знать: основные алгебраические структуры и их свойства.
Б.1.17 Языки программирования	Знать: основные принципы объектно-ориентированного программирования.

4. Время проведения практики

Время проведения практики (номер уч. недели в соответствии с графиком) с 44 по 47

5. Структура практики

Общая трудоемкость практики составляет зачетных единиц 6, часов 216, недель 4.

№ раздела (этапа)	Наименование разделов (этапов) практики	Кол-во часов	Форма текущего контроля
1	Установочные занятия	6	Проверка отчета по практике
2	Линейные рекуррентные последовательности	90	Проверка отчета по практике
3	Реализация поточного шифрования на основе линейных рекуррентных последовательностей	100	Проверка отчета по практике
4	Составление отчета и заполнение дневника практики	20	Проверка отчета по практике

6. Содержание практики

№ раздела (этапа)	Наименование или краткое содержание вида работ на практике	Кол-во часов
1	Установочные лекции по теме и порядку проведения практики	6
2	Изучение линейных рекуррентных последовательностей и решение индивидуальных заданий	90
3	Изучение поточного шифрование и реализация поточного шифрование на основе линейных рекуррентных последовательностей	100
4	Составление отчета и заполнение дневника практики	20

7. Формы отчетности по практике

По окончанию практики, студент предоставляет на кафедру пакет документов, который включает в себя:
- дневник прохождения практики, включая индивидуальное задание и характеристику работы практиканта организацией;
- отчет о прохождении практики.

Формы документов утверждены распоряжением заведующего кафедрой от 31.08.2016 №308-03-04.

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Форма итогового контроля – дифференцированный зачет.

8.1. Паспорт фонда оценочных средств

Наименование разделов практики	Код контролируемой компетенции (или ее части)	Вид контроля
Все разделы	ОПК-2 способностью применять	Дифференцированный

	соответствующий математический аппарат для решения профессиональных задач	зачет
Все разделы	ОК-8 способностью к самоорганизации и самообразованию	Проверка отчета о прохождении практики
Реализация поточного шифрования на основе линейных рекуррентных последовательностей	ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Дифференцированный зачет
Реализация поточного шифрования на основе линейных рекуррентных последовательностей	ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Проверка отчета о прохождении практики
Линейные рекуррентные последовательности	ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач	Проверка отчета о прохождении практики

8.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Дифференцированный зачет	К зачету допускаются студенты, представившие заверенные по месту проведения практики Дневник прохождения практики (включающий индивидуальное задание и характеристику работы практиканта организацией) и Отчет о прохождении практики. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена	Отлично: величина рейтинга обучающегося 85-100% Хорошо: величина рейтинга обучающегося 75-84 % Удовлетворительно: величина рейтинга обучающегося 60-74 % Неудовлетворительно: величина рейтинга обучающегося 0-59%

	приказом ректора от 24.05.2019 г. № 179). Зачет проводится в устной форме в виде защиты представленного Отчета о прохождении практики, в ходе которого студент отвечает на поставленные вопросы об особенностях прохождения практики. Показатели оценивания. Своевременность представления документов: 3 балла - документы представлены в установленные сроки; 2 - балла документы представлены в течение недели после установленного срока; 1 балл - срок задержки представления документов более одной недели. Характеристика работы практиканта: 3 балла - замечаний по прохождению студентом практики не имеется; 2 балла - по прохождению практики имеются замечания непринципиального характера; 1 балл - в характеристике имеются замечания принципиального характер в отношении личных и деловых качеств студента. Защита отчета: 3 балла - при защите студент показывает глубокое знание вопросов, изученных в соответствии с заданием на практику, свободно оперирует данными, уверенно отвечает на вопросы об особенностях прохождения практики; 2 балла – при защите студент в целом показывает знание проблематики практики, однако не вполне уверенно отвечает на дополнительные вопросы; 1 балл – при защите студент проявляет неуверенность, показывает слабое знание объекта прохождения практики. Максимальное количество баллов – 9.	
Проверка отчета о прохождении практики	При оценивании результатов учебной деятельности	Зачтено: Рейтинг обучающегося за

	обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания. 3 балла – отчет содержит логичное, последовательное изложение материала с соответствующими выводами и обоснованными положениями; 2 балла – отчет содержит в целом грамотно изложенную теоретическую главу, однако с не вполне обоснованными выводами; 1 балл – документ базируется на практическом материале, но имеет поверхностный анализ, просматривается непоследовательность изложения материала, представлены необоснованные выводы. Максимальное количество баллов - 3. Весовой коэффициент - 2.	мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %

8.3. Примерный перечень индивидуальных заданий

7. Найти минимальный многочлен линейной рекуррентной последовательности. максимального периода.
8. Разложить многочлены на неприводимые множители над полем Fpc помощью алгоритма Кантора-Цассенхауза.
1. Разложить характеристический многочлен f(x) рекуррентной последовательности на неприводимые множители над полем F2 с помощью алгоритма Берлекэмпа.
10. Реализовать поточное шифрование на основе комбинированной линейной рекуррентной последовательности над полем Fpco сложностью перебора ключа порядка w, вычислить максимальный период линейной рекуррентной последовательности.
3. Вычислить порядок матрицы рекуррентной последовательности, используя нормальную жорданову форму.
6. Проверить, является ли характеристический многочлен f(x) примитивным многочленом и линейная рекуррентная последовательность — последовательностью
5. Найти минимальный период импульсной функции рекуррентной последовательности.
4. Вычислить порядок характеристического многочлена f(x), используя разложение f(x) на неприводимые множители над полем F2.
2. Построить поле разложения многочлена f(x). Найти количество примитивных

элементов и указать примитивный элемент поля разложения. Построить таблицу логарифма Якоби.
9. Вычислить порядки многочленов, используя их разложения на неприводимые множители над полем Fp

9. Учебно-методическое и информационное обеспечение практики

Печатная учебно-методическая документация

а) основная литература:

1. Кепнер, Д. Параллельное программирование в среде MATLAB для многоядерных и многоузловых вычислительных машин [Текст] учеб. пособие Дж. Кепнер ; науч. ред. Д. В. Дубров. - М.: Издательство Московского университета, 2013. - 292 с. ил.
2. Фаддеев, Д. К. Лекции по алгебре [Текст] учебное пособие для вузов по направлениям и специальностям естественнонауч., пед. и техн. наук Д. К. Фаддеев. - 5-е изд., стер. - СПб. и др.: Лань, 2007. - 415,[1] с. ил.

б) дополнительная литература:

1. Патрушева, Е. В. Алгебра и геометрия [Текст] учеб. пособие для самостоят. работы студентов Е. В. Патрушева, Е. А. Неганова, Т. В. Титкова ; Юж.-Урал. гос. ун-т, Каф. Приклад. математика ; ЮУрГУ. - Челябинск: Издательство ЮУрГУ, 2007. - 31, [1] с.
2. Потапов, А. Н. Математическая система MATLAB [Текст] Ч. 1 учеб. пособие для самостоят. работы А. Н. Потапов, Е. М. Уфимцев ; Юж.-Урал. гос. ун-т, Каф. Строительная механика ; ЮУрГУ. - Челябинск: Издательство ЮУрГУ, 2009. - 73, [2] с. ил. электрон. версия

из них методические указания для самостоятельной работы студента:

1. Ручай, Алексей Николаевич. Линейные рекуррентные последовательности в MATLAB [Текст] : практикум / А. Н. Ручай. – Челябинск : Издательство Челябинского государственного университета, 2015. - 99 с

Электронная учебно-методическая документация

Нет

10. Информационные технологии, используемые при проведении практики

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)
3. Math Works-MATLAB, Simulink R2014b(бессрочно)
4. Python Software Foundation-Python (бессрочно)
5. -Python(бессрочно)
6. Microsoft-Visual Studio(бессрочно)

Перечень используемых информационных справочных систем:

1. -База данных ВИНИТИ РАН(бессрочно)

11. Материально-техническое обеспечение практики

Место прохождения практики	Адрес места прохождения	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, обеспечивающие прохождение практики
Кафедра "Защита информации" ЮУрГУ	454080, Челябинск, Ленина, 87	Компьютерный класс