ПРИЛОЖЕНИЕ № 3

к Порядку организации

практической подготовки обучающихся,

утверждённому приказом от

«\_\_\_\_»\_\_\_\_\_\_\_20\_\_\_г. № \_\_\_\_\_\_\_\_\_\_\_

Федеральное государственное автономное образовательное  
учреждение высшего образования   
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт математики, механики и компьютерных наук им И.И. Воровича

*структурное подразделение*

*01.03.02 Прикладная математика и информатика*

*специальность/направление подготовки (код, наименование)*

**ОТЧЁТ**

**о прохождении практики**

обучающегося 2 курса

Фамилия \_\_\_\_\_*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*Горшков*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

Имя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Андрей\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Отчество (при наличии) \_\_\_\_\_\_\_\_\_\_\_Андреевич\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Место практики Институт математики, механики и компьютерных наук им И.И. Воровича

*наименование профильной организации /структурного подразделения Университета*

Вид практики: учебная

*учебная/производственная*

Тип практики: учебная

*указывается в соответствии с ОПОП*

Способ проведения практики: стационарная

*стационарная/выездная*

Сроки прохождения практики: *с \_\_29.06.2021\_\_\_\_\_\_\_\_ по \_\_\_\_\_12.07.2021\_\_\_\_\_\_\_\_\_*\_\_

***Задание обучающегося на практику согласовано\*:***

|  |  |
| --- | --- |
| Руководитель практики  от Университета  Баглий Антон Павлович  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ подпись, Ф.И.О. | Руководитель практики  от профильной организации  подпись, Ф.И.О. |

**I. ЗАДАНИЕ ОБУЧАЮЩЕГОСЯ НА ПРАКТИКУ**

1. Знакомство с платой PYNQ-Z2 и реализация учебных примеров

2. Анализ проектов для ОС PYNQ с открытым исходным кодом, реализующих протокол шифрования AES

3. Сравнение AES и ГОСТ 28147-89

**II. ИНСТРУКТАЖ ПО ОЗНАКОМЛЕНИЮ С ТРЕБОВАНИЯМИ ОХРАНЫ ТРУДА, ТЕХНИКИ БЕЗОПАСНОСТИ, ПОЖАРНОЙ БЕЗОПАСНОСТИ, ПРАВИЛАМ ВНУТРЕННЕГО РАСПОРЯДКА**

|  |  |  |
| --- | --- | --- |
|  | **Инструктаж проведен** | **Ознакомлен** |
| по требованиям охраны труда | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись и Ф.И.О руководителя практики от Университета,)*  «29» июня 2021г. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись и Ф.И.О. обучающегося)*  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. |
| по технике безопасности |
| по пожарной безопасности |
| по правилам внутреннего трудового распорядка |

**III. ДНЕВНИК ПРАКТИКИ**

|  |  |
| --- | --- |
| Дата | Выполненные мероприятия в соответствии с заданием на практику |
| 29.06.21 | Прослушивание инструктажа по технике безопасности, заполнение журнала по технике безопасности. |
| 30.06.21 | Прослушивание вводных лекций. Получение индивидуальных заданий. Консультации по заданиям. |
| 30.06.21 | Знакомство с платой PYNQ Z2, загрузка прошивки на SD-карту и запуск тестовых примеров |
| 01.07.21 | Знакомство с алгоритмами шифрования AES и ГОСТ 28147-89. Проведение архитектурного сравнения данных алгоритмов |
| 02.07.21 | Знакомство с Vivado HLS, изучение принципов работы ПЛИС и методов высокоуровневого синтеза. Оценка возможности разработки алгоритма ГОСТ 28147-89 на ПЛИС |
| 03.07.21 | Проведение тестов времени выполнения алгоритмов AES и ГОСТ 28147-89 на ПК |
| 04.07.21 | Проведение тестов времени выполнения алгоритма AES на PYNQ Z2. Подсчёт вероятного времени выполнения алгоритма ГОСТ 28147-89. Оценка целесообразности использования ПЛИС для данного проекта. |
| 05.07.21 | Реализация алгоритма ГОСТ 28147-89 на PYNQ Z2 с использованием HLS. |
| 09.07.21 | Заполнение дневника и отчета об учебной практике. Защита работы. |
|  |  |

**IV. АНАЛИЗ ПРОВЕДЁННОЙ РАБОТЫ В ПЕРИОД ПРОХОЖДЕНИЯ ПРАКТИКИ ОБУЧАЮЩИМСЯ**

*Раздел заполняется обучающимся в соответствии со спецификой практики (может содержать таблицы, графики, статистические данные и т.п.)*

|  |  |  |
| --- | --- | --- |
| № п/п | Выполненные мероприятия в соответствии с заданием на практику | Анализ проведенной работы |
| 1 | Знакомство с платой PYNQ-Z2 и реализация учебных примеров | На плату PYNQ Z2 был установлен необходимый образ дистрибутива Linux. Разобраны принципы работы платы и ОС, а также ПЛИС. Реализованы проекты-примеры для знакомства с платой |
| 2 | Анализ проектов для ОС PYNQ с открытым исходным кодом, реализующих протокол шифрования AES | Были найдены подходящие для рассмотрения проекты, реализующие протокол шифрования AES и отредактированы для использования на фреймворке PYNQ. Был изучен HLS для разработки под ПЛИС и анализа алгоритма |
| 3 | Сравнение AES и ГОСТ 28147-89 | Было проведено сравнение алгоритмов AES и ГОСТ 28147-89, а также выполнены тесты скорости работы для определения целесообразности использования ПЛИС в данной задаче |

Постановки задачи

Познакомиться с алгоритмами шифрования AES и ГОСТ 28147-89 с целью определения целесообразности использования фреймворка PYNQ для реализации потокового шифрования на ГОСТ 28147-89. Протестировать реализацию алгоритма шифрования AES на фреймворке PYNQ с использованием отладочной платы PYNQ Z2. Сравнить пропускную способность реализаций алгоритма AES для PC и PYNQ Z2. Спрогнозировать пропускную способность ГОСТ 28147-89 по результатам тестирования версии на PC. Описать возможность реализации ГОСТ 28147-89 на фреймворке PYNQ и способы оптимизации вычислений.

Изучение алгоритмов шифрования

Изучение алгоритмов шифрования происходило по источникам [1][2], а также по реализациям с открытым исходным кодом [3][4].

AES – симметричный алгоритм блочного шифрования, построенный на подстановочно-перестановочной сети, принятый в качестве стандарта шифрования правительством США. Оперирует блоками по 128 бит и ключом длиной 128, 192 или 256 бит и производит 10, 12 или 14 раундов шифрования в зависимости от длины ключа. За один раунд AES шифрует один блок данных, производя в каждом раунде сложение блока с раундовым ключом, байтовую подстановку, побайтовый циклический сдвиг в строках матрицы и матричное умножение.

ГОСТ 28147-89 — российский стандарт симметричного блочного шифрования, принятый в 1989 году. Основан на сети Файстеля. Длина блока – 64 бит, длина ключа фиксирована и составляет 256 бит. Производит 32 раунда шифрования, в каждом из которых шифруется половина блока данных, производя комбинирование входной половины блока с раундовым ключом – сложения их по модулю , подстановки, выполняемой независимо в восьми 4-битовых группах, и битовой перестановки. Раундовый ключ генерируется путём разбиения входного ключа на блоки по 32 бита. Для раундов 1-8, 9-16, 7-24 используются соответствующие элементы входного ключа, а для раундов 25-32 ключ используется в обратном порядке.

Оба алгоритма имеют несколько режимов:

1. ECB – простая замена. Каждый блок шифруется отдельно от остальных, поэтому два одинаковых блока будут зашифрованы идентичным образом.
2. CBC – сцепление блоков. Каждый блок открытого текста складывается по модулю два с предыдущим блоком шифротекста, а затем шифруется. Для уникальности каждого блока используется синхропосылка. Таким образом, каждый блок шифротекста зависит от всех обработанных блоков открытого текста.
3. SM – режим гаммирования. Открытый текст складывается по модулю два с гаммой шифра. Гамма шифра генерируется с помощью случайного вектора инициализации (синхропосылки) путём шифрования в режиме простой замены. В этом режиме процессы шифрования и дешифрования симметричны.
4. CFB – режим гаммирования с обратной связью. Превращает блочный шифр в самосинхронизирующийся поточный шифр. Шифрование следующего блока открытого текста происходит путём сложения по модулю 2 перешифрованного блочным шифром результата шифрования предыдущего блока.
5. OFB – режим гаммирования с обратной связью по выходу. Преобразует блочный шифр в синхронный поточный шифр путём сложения по модулю два генерируемого ключевого блока с блоками открытого текста.
6. CTR – режим счётчика. Ключевой блок генерируется путем зашифрования последовательных значений счетчика и затем складывается по модулю два с открытым текстом или шифротекстом. Операции шифрования и дешифрования могут выполняться параллельно, так как для очередного блока необходимо знать только значение счетчика. Вследствие того, что операция сложения по модулю два является симметричной, процесс шифрования и расшифрования выглядит одинаково.

Из сказанного можно сделать вывод, что по основным параметрам криптостойкости ни один алгоритм не обладает особым преимуществом перед другим. Несмотря на архитектурное различие ГОСТ 28147-89 и AES, их основные рабочие параметры сопоставимы.

Для реализации алгоритмов шифрования для PYNQ Z2 можно воспользоваться высокоуровневым синтезом (High-level synthesis, HLS). Данный метод позволяет синтезировать язык высокого уровня (в данном случае C++) в конфигурацию для ПЛИС, что позволяет использовать преимущества ПЛИС, такие как высокая параллельность вычислений и конвейеризацию обработки данных, при достаточно высоком уровне абстракции.

Программная реализация

Для изучения работы с платой PYNQ Z2, продемонстрированной на рисунке 1, были использованы материалы из официальной документации [5][6].

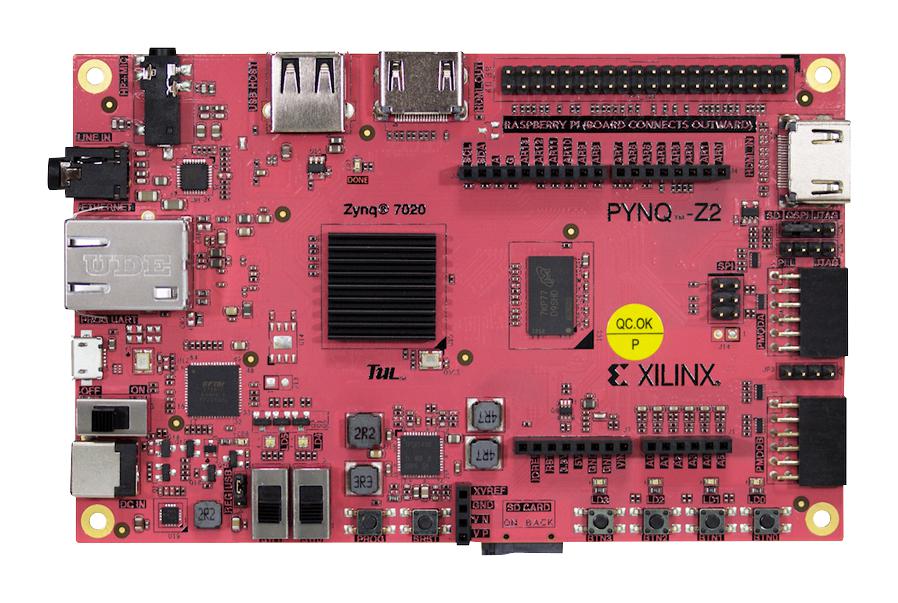


Рисунок 1

Данная плата состоит из ПЛИС и микроконтроллера Zynq 7020, выполненного по архитектуре ARM. Также в стандартную поставку входит образ специально подготовленного дистрибутива Linux. Данная плата уникальна тем, что для программирования использует Jupyter Notebook. Производителем также выполнена работа по написанию библиотек на языке Python для управления и прошивки ПЛИС, что позволило выполнять аппаратное ускорение кода.

Для проведения экспериментов по замеру пропускной способности были использованы реализации алгоритмов шифрования AES и ГОСТ 28147-89 с открытым исходным кодом для архитектуры x86-64 [3], [4]. Реализация AES для архитектуры x86-64 реализует несколько функций:

1. ECB. Отвечают функции EncryptECB/DecryptECB, принимающие исходный текст, его длину и ключ.
2. CBC. Режим реализован функциями EncryptCBC/ DecryptCBC. Принимают исходный текст, его длину, ключ и вектор инициализаци.
3. CFB. Реализовано функциями EncryptCFB/DecryptCFB. Принимают исходный текст, его длину, ключ и вектор инициализации.

Все методы описаны в классе AES, который также содержит вспомогательные методы, такие как: добавление нулей к блоку данных и ключу (PaddingNulls, KeyExpansion), шифрование/дешифрование одного блока данных (EncryptBlock, DecryptBlock), генерация ключа раунда (AddRoundKey), а также функции побитовых сдвигов, сложений по модулю 2 блоков данных и умножения матриц (XorBlocks, XorWords, ShiftRow).

Реализация ГОСТ 28147-89 также содержит несколько режимов:

1. ECB. Реализовано функцией GOST\_Encrypt\_SR, которая принимает данные для шифрования, их размер, режим(шифрование/дешифрование), таблицу замен и ключ.
2. SM. Реализовано функцией GOST\_Encrypt\_G\_Data, которая принимает данные для шифрования, их размер, синхропосылку, таблицу замен и ключ.
3. CFB. Реализовано функцией GOST\_Encrypt\_GF\_Data, которая принимает данные для шифрования, их размер, синхропосылку, режим(шифрование/дешифрование), таблицу замен и ключ.

Помимо описанных функций, реализация содержит несколько вспомогательных: подготовка синхропосылки в различных режимах (GOST\_Crypt\_G\_PS, GOST\_Crypt\_GF\_Prepare\_S), расчёт имитовставки (GOST\_Imitta). Блок данных хранится в union GOST\_Data\_Part для разбиения на восемь 8-битных блоков или двух 32-битных.

Для измерения времени работы алгоритмов используется библиотека chrono из стандартной библиотеки std и функция std::chrono::steady\_clock::now(). Замеры времени проводились после считывания данных из файлов в буфер. При этом были использованы файлы размером 200 килобайт, 1 мегабайт, 10 мегабайт и 100 мегабайт. Важно отметить, что в данных реализациях не используется аппаратное ускорение на уровне ассемблерных инструкций, что существенно влияет на их скорость работы, но не является существенным в рамках данной работы.

Реализация AES для PYNQ Z2 состоит из кода на языке C++, подвергаемому высокоуровневому синтезу для ПЛИС, и из кода на языке Python, выполняемом на ARM процессоре.

Шифрование реализовано функцией AES\_En\_De, которая принимает входящий поток данных собственного типа my\_stream\_type, состоящего из собственно данных и бита завершения (необходимо для использования на ПЛИС через интерфейс AXI), выходящий поток такого же типа, длину потока и ключ. Также реализовано несколько вспомогательных функций, таких как: конвертеры данных (convertToIntArray, getNumFromSBox, getIntFromChar, getWordFromStrб getArrayFrom4W), сплиттеры (splitIntToArray, mergeArrayToInt), побитовые сдвиги и сложение по модулю 2 (shiftRows, deShiftRows, GFMul2).

Для работы HLS в главной функции AES\_En\_De используются директивы препроцессора #pragma HLS interface, описанные в [6], которые указывают порты для ПЛИС и некоторые методы оптимизации, такие как распараллеливание. Также в состав Vivado HLS входят библиотеки, использование которых позволяет максимально оптимизировать код [7]. Они содержат описания удобных для использования типов данных, таких как ap\_int<N>, hls::stream<T>, hls::Scalar<T, U>.

Код на Python содержит функции для доступа к ПЛИС. Для доступа к портам ввода-вывода используется объект MMIO, через который по DMA отправляются необходимые данные в IP-блок.

Описание методов класса AES:

1. call\_AES\_En\_De передаёт входной текст и ключ в IP-блок и получает результат;
2. expand\_to\_128b расширяет входные данные до 128 байт, заполняя нулями;
3. string\_AES\_En\_De вызывает call\_AES\_En\_De для шифрования строки, но предварительно делит её на блоки, если она больше максимального буфера IP-блока (345600 символов);
4. file\_AES\_En\_De служит для шифрования файла;
5. image\_AES\_En\_De – для шифрование изображения формата PIL.

Для измерения времени используется метод time() из стандартного модуля time.

Анализ результатов эксперимента

Изучение алгоритмов шифрования ГОСТ 28147‑89 и AES показало, что рабочие параметры сопоставимы, несмотря на различную архитектуру, что позволяет сравнить их между собой и подсчитать предполагаемую скорость работы ГОСТ 28147‑89 в том же режиме на PYNQ Z2.

Результаты проведенных экспериментов по измерению пропускной способности приведены ниже в таблицах. Было произведено несколько замеров, результаты которых незначительно различались, что обусловлено работой операционной системы и встроенного планировщика задач.

|  |  |  |
| --- | --- | --- |
| **Размер данных** | **Время выполнения, мс** | **Скорость, мбит/с** |
| 200 кбайт | 18 | 88.8 |
| 1 мбайт | 94 | 87.14 |
| 10 мбайт | 936 | 87.52 |
| 100 мбайт | 9252 | 88.53 |

1Результат теста времени выполнения шифрования по алгоритму ГОСТ 28147-89 на ПК (Intel Core i5)

|  |  |  |
| --- | --- | --- |
| **Размер данных** | **Время выполнения, мс** | **Скорость, мбит/с** |
| 200 кбайт | 67 | 23.8 |
| 1 мбайт | 340 | 24.08 |
| 10 мбайт | 3356 | 26.80 |
| 100 мбайт | 33498 | 24.40 |

2Результат эксперимента по измерению времени шифрования по алгоритму AES на ПК (Intel Core i5)

Как видно из результатов, скорость работы алгоритма ГОСТ 28147-89 превосходит скорость AES примерно в три раза. При это реализация AES с использованием аппаратного ускорения на ПЛИС дает прирост в 75%:

|  |  |  |
| --- | --- | --- |
| **Размер данных** | **Время выполнения, мс** | **Скорость, мбит/с** |
| 200 кбайт | 51 | 31.36 |
| 1 мбайт | 254 | 32.76 |
| 10 мбайт | 3738 | 21.62 |
| 100 мбайт | 21701 | 32.38 |

3Результат теста времени выполнения шифрования для алгоритма AES на PYNQ Z2 с использованием ПЛИС

Проведенные эксперименты показали, что пропускная способность при шифровании файлов размером 1 и 10 мбайт стабильно ниже, чем 100 мбайт. Предположительно, это связано с алгоритмами взаимодействия между ARM и ПЛИС и управления памятью, но точную причину выяснить не получилось в силу ограниченного времени на проведение исследования.

Данный эксперимент также был произведен на плате PYNQ Z2 без аппаратного ускорения на ПЛИС. Результаты представлены в следующей таблице. По ним видно, что использование аппаратного ускорения увеличивает пропускную способность примерно в 22 раза.

|  |  |  |
| --- | --- | --- |
| **Размер данных** | **Время выполнения, мс** | **Скорость, мбит/с** |
| 200 кбайт | 1059 | 1.50 |
| 1 мбайт | 5475 | 1.46 |
| 10 мбайт | 98240 | 1.48 |
| 100 мбайт | 545992 | 1.46 |

4Результат теста времени выполнения шифрования для алгоритма AES на PYNQ Z2 без использования ПЛИС

Так как алгоритмы шифрования похожи по своему внутреннему устройству, из собранных данных методом пропорции можно сделать выводы о приблизительной скорости шифрования при реализации ГОСТ 28147‑89 на PYNQ Z2. Формула и проведенные расчеты представлены ниже. Очевидно, что такое сравнение может дать только приблизительный результат, но в рамках данного исследования больше и не требуется.

|  |  |
| --- | --- |
| **Размер данных** | **Скорость, Mbps** |
| 200 кб | 117.00 |
| 1 мб | 118.55 |
| 10 мб | 70.60 |
| 100 мб | 117.47 |

5Вероятная скорость работы алгоритма "Магма" на PYNQ Z2 с использованием ПЛИС

В случае шифрования 200 килобайтного, 1 мегабайтного и 100 мегабайтного файлов предполагаемая скорость работы алгоритма на PYNQ Z2 превосходит скорость работы на PC и при этом может быть реализовано в форм-факторе компактного низкопотребляющего устройства. При этом использование алгоритмов оптимизации и всех возможностей ПЛИС, таких как распараллеливание, оптимизации циклов, оптимизации массивов, а также использование языка низкого уровня вместо Python для управления ПЛИС, даст возможность увеличить скорость работы. Таким образом, использование ПЛИС для аппаратного ускорения алгоритма шифрования ГОСТ 28147‑89 целесообразно.

Выводы

Все поставленные задачи успешно выполнены. Также были произведены попытки портирования реализации алгоритма ГОСТ 28147‑89 с PC на PYNQ, однако, полученный IP-блок не удалось подключить к интерфейсу AXI DMA, без которого невозможно передавать блоки данных.

Список использованных источников

1. Википедия, описание ГОСТа 28147-89 –

[ГОСТ 28147-89 — Википедия (wikipedia.org)](https://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_28147-89)

1. Цикл статей о «Магме» на Хабре –

[ГОСТ 28147-89 (Часть 1. Введение и общие принципы) / Хабр (habr.com)](https://habr.com/ru/post/80967/)

1. Репозиторий с исходным кодом реализации шифра AES на C++ –

[SergeyBel/AES: C++ AES implementation (github.com)](https://github.com/SergeyBel/AES)

1. Репозиторий с исходным кодом реализации шифра «Магма» на C++ -

[yolomachine/Magma: Russian government standard symmetric key block cipher, defined in a standard GOST 28147-89. Implemented in educational causes (github.com)](https://github.com/yolomachine/Magma)

1. Документация к PYNQ Z2 –

[Getting Started — Python productivity for Zynq (Pynq)](https://pynq.readthedocs.io/en/latest/getting_started.html)

1. Документация к Vivado HLS

[Introduction (xilinx.com)](https://www.xilinx.com/html_docs/xilinx2017_4/sdaccel_doc/gkv1510957295794.html)

1. Библиотека ap\_int

[ThesisCode/ap\_int.h at master · joshuaspence/ThesisCode (github.com)](https://github.com/joshuaspence/ThesisCode/blob/master/TopN_Outlier_Pruning_Block/include/autoesl/ap_int.h)

**ОТЗЫВ РУКОВОДИТЕЛЯ ПРАКТИКИ ОТ ПРОФИЛЬНОЙ ОРГАНИЗАЦИИ \***

*Отзыв оформляется руководителем практики от профильной организации в свободной форме с указанием полноты, своевременности и качества проведенной обучающимся работы*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Руководитель практики

от профильной организации / Баглий Антон Павлович

подпись Ф.И.О.

**ОТЗЫВ РУКОВОДИТЕЛЯ ПРАКТИКИ от УНИВЕРСИТЕТА**

*Отзыв оформляется руководителем практики от Университета в свободной форме с указанием полноты, своевременности и качества проведенной обучающимся работы*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*зачтено/отлично/хорошо/удовлетворительно*

Руководитель практики

от Университета / Баглий Антон Павлович

подпись Ф.И.О.

***Примечания:***

1. Отчёт о прохождении практики является основным рабочим и отчётным документом обучающегося в период прохождения практики.
2. Обучающийся заполняет отчёт о прохождении практики регулярно в течение всего периода практики.
3. Заполненный отчёт о прохождении практики обучающийся сдает руководителю практики от Университета по завершению практики в соответствии с графиком учебного процесса.
4. Отчёты о прохождении практики обучающихся хранятся на соответствующей кафедре в течение всего периода реализации образовательной программы.

\*Заполняется в случае проведения практики в профильной организации