**Федеральное государственное образовательное бюджетное учреждение высшего образования**

**«Финансовый университет при Правительстве Российской Федерации»**

**Колледж информатики и программирования**

Группа: 4ПКС-115

**Отчет по производственной практике**

**(преддипломной)**

**Руководитель практики от предприятия**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Руководитель практики от колледжа**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Студент**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Оценка** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.2019

2019

Содержание

[Введение 3](#_Toc8909191)

[1 Общая часть 5](#_Toc8909192)

[1.1 Описание структурного подразделения организации 5](#_Toc8909193)

[1.2 Технические, инструментальные и программные средства, используемые в подразделении для выполнения работ 5](#_Toc8909194)

[2 Исследовательская часть 6](#_Toc8909195)

[2.1 Предпроектное обследование предметной области 6](#_Toc8909196)

[2.2 Характеристика инструментальных средств разработки 8](#_Toc8909197)

[Заключение 12](#_Toc8909198)

[Список использованных источников 13](#_Toc8909199)

# Введение

ПАО «НПП Сапфир» является базовым предприятием российской оборонной промышленности. Оно сосредоточило свои усилия на научно-производственном направлении по созданию радиационно-стойких КМОП, КНС и БИС, технология изготовления которых имеет статус Федерального уровня.

ПАО «НПП Сапфир» осуществляет поставки микропроцессоров для нужд Роскосмоса и Минатома Российской Федерации.

Предприятие имеет огромный опыт производства и разработки наукоемкой продукции, применяемой в бортовых системах и вычислительных комплексах баллистических ракет.

Сочетание традиционных и новых направлений в разработках и производстве полупроводниковой электроники, создание законченных изделий и устройств для первоочередных нужд народного хозяйства и обороны страны позволяет НПП «Сапфир» развивать науку и производство России.

При ПАО «НПП Сапфир» на базовой кафедре «Некогерентная оптоэлектроника» проводятся по специальным предметам занятия по специальности 210101 «Микроэлектроника и твердотельная электроника».

Подготовка инженеров проводится в соответствии с действующими Государственными образовательными стандартами.

На производственной базе ПАО «НПП Сапфир» работают множество предприятий малого и среднего бизнеса.

Двадцать из них объединены в созданном в 2005 году Технопарк «Сапфир».

Целью прохождения преддипломной практики является:

* изучение научно-практического материала по разделам ВКР;
* подбор фактического материала на базе организации;
* развитие практических навыков и компетенции в процессе выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой ВКР.

Задачами преддипломной практики являются:

* проведение анализа и обобщения научно-технической информации по теме ВКР;
* подбор фактического материала по теме ВКР с учетом профессиональных модулей и его изучение;
* подготовка плана пояснительной записки к ВКР;
* подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР;
* описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием;
* оформление и сдача отчета по преддипломной практике.

Вопросы, подлежащие изучению.

* литературные источники по разрабатываемой теме с целью их использования при выполнении выпускной работы;
* методы исследования и проведения работ, анализа и обработки данных;
* информационные технологии и технические средства в профессиональной деятельности;
* программные продукты, относящиеся к профессиональной сфере;
* критерии выбора, сравнения и оценки эффективности решений по защите информации;
* требования к оформлению научно-технической документации.

# Общая часть

### Описание структурного подразделения организации

Преддипломная практика проходила в конструкторско-технологическом отделе ПАО «НПП Сапфир». Основной задачей этого отдела является разработка программ для контроля качества произведённой продукции.

Измерения контроля качества проводятся на специальных установках, на которых микросхемы подвергаются испытаниям в самых различных условиях, полученные в ходе испытаний данные сравнивают с эталонными и вычисляют процент их отклонения. Далее микросхемы отправляют на семидневную токовую тренировку, в этот промежуток времени микросхемы подвергаются нагрузкам в различных температурных условиях, а затем измерения проводятся снова.

Таким образом отбивается продукция высшего качества и определяются недочёты, исправление которых в дальнейшем позволяет совершенствовать будущие микросхемы.

### Технические, инструментальные и программные средства, используемые в подразделении для выполнения работ

Практиканту было необходимо изучить научно-практический материал по разделам ВКР, а также подобрать фактический материал на базе организации.

Для выполнения поставленной задачи было предоставлено:

* рабочий компьютер;
* научная литература в соответствии с темой ВКР.

## Исследовательская часть

### Предпроектное обследование предметной области

Криптография – это наука, изучающая способы сокрытия данных и обеспечения их конфиденциальности. Это одна из старейших наук и ее история насчитывает четыре тысячелетия. Сам термин «криптография» образовался от двух древнегреческих слов «крипто» – скрытый, «графо» – пишу.

До 1975 года криптография представляла собой шифровальный метод с секретным ключом, который предоставлял доступ к расшифровке данных. Позже начался период ее современного развития и были разработаны методы криптографии с открытым ключом, которые может передаваться по открытым каналам связи и использоваться для проверки данных.

Современная прикладная криптография представляет собой науку, образованную на стыке математики и информатики. Смежной наукой криптографии считается криптоанализ. Криптография и криптоанализ тесно взаимосвязаны между собой, только в последнем случае изучаются способы расшифровки сокрытой информации.

С модификацией до открытого ключа криптография получила более широкое распространение и стала применяться частными лицами и коммерческими организациями, а в 2009 году на ее основе была выпущена первая криптовалюта Биткоин. До этого времени она считалась прерогативой государственных органов правления.

В основе криптографических систем лежат различные виды криптографии. Всего различаю четыре основных криптографических примитива:

* симметричное шифрование – данный метод предотвращает перехват данных третьими лицами и базируется на том, что отправитель и получатель данных имеет одинаковые ключи для разгадки шифра;
* асимметричное шифрование – в этом методе задействованы открытый и секретный ключ. Ключи взаимосвязаны – информация, зашифрованная открытым ключом, может быть раскрыта только связанным с ним секретным ключом. Применять для разгадки ключи из разных пар невозможно, поскольку они связаны между собой математической зависимостью;
* хэширование – метод основывается на преобразовании исходной информации в байты заданного образца. Преобразование информации называется хэш-функцией, а полученный результат хэш-кодом. Все хэш-коды имеют уникальную последовательность символов;
* электронная подпись – это преобразование информации с использованием закрытого ключа, позволяющее подтвердить подлинность документа и отсутствие искажений данных.

Изначально криптография использовалась правительством для безопасного хранения или передачи документов. Современные же асимметричные алгоритмы шифрования получили более широкое применение в сфере IT-безопасности, а симметричные методы сейчас применяются преимущественно для предотвращения несанкционированного доступа к информации во время хранения.

В частности, криптографические методы применяются для:

* безопасного хранения информации коммерческими и частными лицами;
* реализации систем цифровой электронной подписи;
* подтверждения подлинности сертификатов;
* защищенной передачи данных онлайн по открытым каналам связи.

Криптография является важной составляющей современного мира и необходима в первую очередь для сохранения персональных данных и важной информации. С момента появления она прошла множество модификаций и сейчас представляет собой систему безопасности, которая практически не может быть взломана. Переоценить ее возможности для человечества сложно. Современные методы криптографии применяются практически во всех отраслях, в которых присутствует необходимость безопасной передачи или хранения данных.

В связи с описанным выше передо мной была поставлена задача разработать программу для шифрования файлов и их дешифровке. Для этого были выбраны следующие алгоритмы:

* шифр одноалфавитной замены;
* шифр много алфавитной замены;
* код Фрэнсиса Бэкона;
* XOR;
* тарабарщина;
* RSA;
* DSA.

### Характеристика инструментальных средств разработки

Для написания программы было решено использовать среду программирования Visual Studio 2017 и язык программирования C# версии 7.0. NET Framework 4.7.1.

Для построения схем и диаграмм при составлении технического задания и сопровождающей документации было решено использовать Draw.io. Draw.io — это сервис, предназначенный для формирования диаграмм и схем. Сервис разделён на три части — меню, панель объектов и сам документ.

С помощью веб-сервиса Draw.io можно создавать:

* диаграммы.
* UML-модели.
* вставка в диаграмму изображений.
* графики.
* блок-схемы.
* формы.
* другое.

Для начала пользователь может выбрать объект из панели, просмотрев категории, и перенести мышью объект в документ. Для соединения объектов блок-схемы необходимо выделить второй объект и навести указателем на первый, далее появится зелёный флажок и с помощью него выполняется перетаскивание.

В меню сервиса диаграмму или схему можно отформатировать следующими настройками:

* стиль шрифта.
* цвет фона документа или объектов.
* тени и степень прозрачности.
* цвет и толщина линий.
* заливка и градиент.

Также доступен экспорт готовых схем в изображение (PNG, GIF, JPG, PDF) и синхронизация полученных документов с Google Диском.

Visual Studio 2017 – является продуктом из линейки компании Microsoft, включающих интегрированную среду разработки программного обеспечения и ряд других инструментальных средств. Продукты из этой линейки позволяют разрабатывать как консольные приложения, так и приложения с графическим интерфейсом.

Visual Studio 2017 включает в себя редактор исходного кода с поддержкой технологии IntelliSense и возможностью простейшего рефакторинга кода. Встроенный отладчик может работать как отладчик уровня исходного кода, так и как отладчик машинного уровня. Остальные встраиваемые инструменты включают в себя редактор форм для упрощения создания графического интерфейса приложения, веб-редактор, дизайнер классов и дизайнер схемы базы данных.

Язык программирования C#, используемый в разработке приложения, является объектно-ориентированным. C# относится к семье языков с C-подобным синтаксисом, его синтаксис наиболее близок к C++ и Java. Язык имеет статическую типизацию, поддерживает полиморфизм, перегрузку операторов (в том числе операторов явного и неявного приведения типа), делегаты, атрибуты, события, свойства, обобщённые типы и методы, итераторы, анонимные функции с поддержкой замыканий, LINQ, исключения, комментарии в формате XML.

Ниже перечислены основные достоинства языка С#:

* является объектно-ориентированным языком, где типы, встроенные в язык, представлены классами;
* предоставляет возможности наследования и универсализации;
* является наследником языков C/C++, сохраняя лучшие черты этих популярных языков программирования;
* является простым и надёжным, поскольку на C# хотя и допускаются, но не поощряются такие опасные свойства С++, как указатели, адресация, разыменование, адресная арифметика;
* предоставляет возможность создавать многопоточные программы;
* создавался параллельно с каркасом Framework .Net и в полной мере учитывает все его возможности – поддержку как Framework Class Library (FCL), так и Common Language Runtime (CLR);
* благодаря каркасу Framework .Net, ставшему надстройкой над операционной системой, программисты C# получают те же преимущества работы с виртуальной машиной, что и программисты Java. Эффективность кода даже повышается, поскольку исполнительная среда CLR представляет собой компилятор промежуточного языка, в то время как виртуальная Java-машина является интерпретатором байт-кода.

В разрабатываемом программном модуле использованы такие структуры и конструкции языка программирования C#, как:

* классы и вложенные классы;
* перечисления;
* потоки;
* потоки данных;
* перегрузка индексатора.

Одним из ключевых аспектов в современном программировании является многопоточность. Ключевым понятием при работе с многопоточностью является поток. Поток представляет некоторую часть кода программы. При выполнении программы каждому потоку выделяется определенный квант времени. И при помощи многопоточности мы можем выделить в приложении несколько потоков, которые будут выполнять различные задачи одновременно. Благодаря потокам мы можем выделить отправку запроса или любую другую задачу, которая может долго обрабатываться, в отдельный поток. Поэтому клиент-серверные приложения практически не мыслимы без многопоточности.

# Заключение

Во время прохождения производственной преддипломной практики были изучены:

* литературные источники по разрабатываемой теме ВКР с целью их использования при выполнении выпускной работы;
* методы исследования и проведения работ, анализа и обработки данных;
* информационные технологии и технические средства в профессиональной деятельности;
* программные продукты, относящиеся к профессиональной сфере;
* критерии выбора, сравнения и оценки эффективности решений по защите информации;
* требования к оформлению научно-технической документации.

В ходе прохождения преддипломной практики был проведён анализ и обобщение научно-технической информации в соответствии с темой ВКР. Был подобран и изучен фактический материал с учётом профессиональных модулей, а также подготовлен план пояснительной записки ВКР.

Итогами прохождения преддипломной практики является выполнение всех поставленных целей и задач в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

# Список использованных источников

Стандарты

1. ГОСТ 7.1. – 2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления. – М.: ИПК Издательство стандартов, 2004. – 169 с.
2. ГОСТ 7.32 – 2001. Система стандартов по информацию, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления. – М.: ИПК Издательство стандартов, 2001. – 21 с.
3. ГОСТ 7.82 – 2001. Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления. – М.: ИПК Издательство стандартов, 2001. –21 с.
4. Единая система программной документации. – М.: Стандартинформ, 2005. –128 с.

Интернет-ресурсы

1. Документация по Visual Studio – [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/ru-ru/visualstudio/get-started/visual-studio-ide?view=vs-2017
2. Криптография и шифрование данных – всё, что нужно знать – [Электронный ресурс]. – Режим доступа: https://prostocoin.com/blog/cryptography
3. Новые возможности C# 7.0 – [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/ru-ru/dotnet/csharp/whats-new/csharp-7
4. Описание Draw.io – [Электронный ресурс]. – Режим доступа: https://startpack.ru/application/draw-io