Министерство образования Республики Беларусь

Белорусский государственный университет

Факультет радиофизики и компьютерных технологий

Кафедра информатики и компьютерных систем

Отчет о производственной преддипломной практике

Данилина Даниила Алексеевича

студента 4 курса,

специальности

1-98 01 01 «Компьютерная безопасность»

Руководитель практики от организации:

Заместитель начальника отдела компьютерно-технических экспертиз управления компьютерно-технических экспертиз и экспертиз радиоэлектронных устройств главного управления технических экспертиз центрального аппарата Государственного комитета судебных экспертиз Республики Беларусь Шаховец Андрей Александрович

Минск 2022

**Место прохождения практики:** управление компьютерно-технических экспертиз и экспертиз радиоэлектронных устройств главного управления технических экспертиз центрального аппарата Государственного комитета судебных экспертиз Республики Беларусь.

**Срок практики:** с 04 апреля 2022 г. по 30 апреля 2022 г.

**Цель практики:**

1. Изучение в практических условиях методов, применяемых при проведении компьютерно-технических экспертиз. Ознакомление с современным оборудованием и особенностями его использования на предприятии.
2. Работа с научной литературой по тематике дипломной работы, получение навыков работы с алгоритмами шифрования, и анализ результатов экспериментов для включения в дипломную работу.

**Задачи на практику:**

1. Изучение в практических условиях основ организации научно-исследовательских работ, производственной деятельности в центральном аппарате Государственного комитета судебных экспертиз;

2. Изучение особенностей извлечения данных из носителей информации;

3. Использование современных методов восстановления удалённой информации;

4. Приобрести опыт работы с использованием современных методов шифрования информации;

5. Изучить этапы по подготовке и оформление результатов проведения экспертизы (заключения эксперта);

6. Формирование и анализ результатов для включения в дипломную работу.

**Тема дипломной работы**: «Разработка безопасного клиент-серверного приложения для обмена информации на предприятии».

**Введение**

Реальности сегодняшних дней обуславливают неуклонный рост количества различного рода споров, которые становятся объектом рассмотрения в различных инстанциях. Для принятия правильного и справедливого решения тех или иных вопросов просто необходимо привлечения узких специалистов в различных сферах деятельности. Проведение необходимых исследований и дача квалифицированного заключения — цель работы экспертов и экспертных учреждений.

В процессе проведения судебной экспертизы, которая проводится на основе специальных познаний в науке, технике, искусстве или ремесле, полного и объективного исследования обстоятельств дела, устанавливаются фактические данные, имеющие доказательственное значение, что и позволяет решать основной вопрос судопроизводства о виновности (невиновности) лица.

Эксперт зачастую обладает необходимыми знаниями в родственных сферах науки. Так, например, обладая знаниями в областях информационных технологий, эксперт способен проводить исследования компьютерной техники и мобильных устройств. Оба вида исследования предполагают извлечение информации, однако их методы и методы дальнейшего исследования имеют различия.

**Описание этапов выполнения экспертиз**

Первоначальным этапом в исследовании мобильных устройств и компьютерной техники является создание точной копии с носителя информации. Необходимость данного действия заключается в ограничении (полном или частичном) внесения изменений в исследуемый объект. Это делается для уверенности в том, что эксперт намеренно не скрыл некоторые факты. Таким образом с носителей информации ПЭВМ, а также карты памяти различных устройств, делается полная копия содержимого и структуры файловой системы и данных (побитовая копия). Данная копия позволяет провести подробное исследования без дальнейшего участия в этом непосредственного аппаратного объекта исследования. Следует также отметить, что некоторые из методов копирования, каждый из которых использует определённую уязвимость, могут требовать ввода пользовательского пароля.

Вторым этапом исследования информации является анализ ее копии, которая хранится на ПЭВМ эксперта. В начале этого этапа эксперт использует специализированное программное обеспечение для восстановления удаленных данных. В зависимости от поставленных вопросов имеется возможность выгрузки каталогов, в том числе удаленных в удобном виде, а также извлечение информации из баз данных различных приложений. В основном работа автоматизирована, но иногда есть необходимость проверки баз данных вручную.

Заключительный этап – оформление таблицы фотоснимков и заключения эксперта. Ход исследования информации подробно описывается в данном документе и на основании полученных данных формируются ответы на поставленные вопросы. Документ может повлиять на ход дела и доказать, как виновность, так и невиновность подозреваемого. Вот почему эксперт должен быть компетентен в рассмотрении вопросов, по которым он дает ответ используя соответствующие знания в областях, в которых он проводит исследование.

**Разработка безопасного клиент-серверного приложение для шифрованного обмена информацией внутри предприятия.**

В период прохождения преддипломной практики было выполнено индивидуальное задание, заключающееся в анализе задания на дипломное проектирование, проведение поиска научно-технической литературы, а также разработка клиент-серверного приложения.

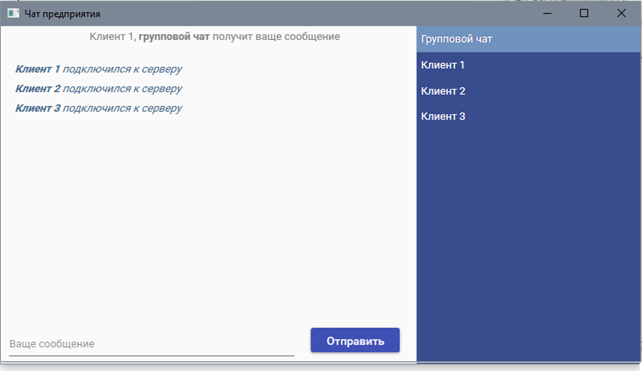
Во время преддипломной практики были изучены аспекты защиты информации на носителях, в том числе способы защищенной передачи данных от одного устройства к другому. Произошло ознакомление с современными алгоритмами шифрования, также с научным руководителем обсуждены возможные инновационные варианты с сфере защиты информации.

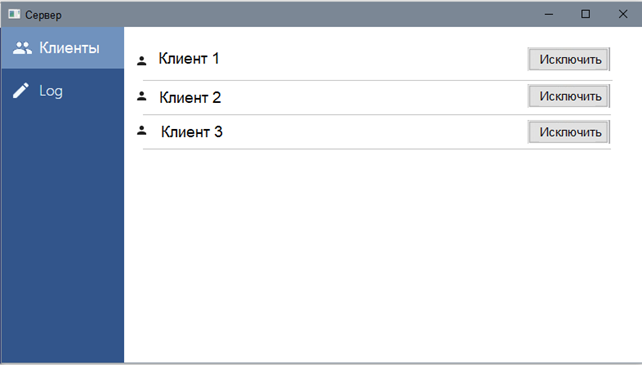
Были изучены программно-технические средства, эксплуатируемые на базе центрального аппарата Государственного комитета судебных экспертиз. В том числе были исследованы на практике такие критерии блочных шифров как:

* параметры ключа: его длина и длина блока, обеспечивающие верхнюю границу безопасности шифра;
* оценка уровня безопасности, основанная на достигнутой в блочном шифре конфиденциальности и полученная после того, как шифр выдержит значительное число попыток криптоанализа на протяжении времени; стойкость математической модели и существования практических способов атак;
* сложность шифра и пригодности к программной или аппаратной реализации. В случае аппаратной реализации сложность шифра может быть оценена в числе использованных вентилей или энергопотреблении. Эти параметры важны для устройств, ограниченных в ресурсах;
* производительность шифра, выраженная в пропускной способности шифра на различных платформах и потребляемой памяти;
* стоимость шифра, которая может быть обусловлена лицензионными требованиями в соответствии с интеллектуальной собственностью;
* гибкость шифра, связанная со способностью поддерживать множество длин ключей и блоков.

За время преддипломной практики был изучен и реализован блочный алгоритм симметричного шифрования ГОСТ 34.12-2015 на языке программирования C#. Основу алгоритма составляет так называемая SP-сеть (подстановочно-перестановочная сеть). Шифр на основе SP-сети получает на вход блок и ключ и совершает несколько чередующихся раундов, состоящих из стадий подстановки и стадий перестановки. Созданы методы для передачи шифрованных сообщения и ключей между клиентами и сервером, для корректного взаимодействия между пользователями приложения.

А так же приняты советы для создания простого в использование интерфейса для пользователя. Программа предназначена для приятного и полезного использования в рабочее время. Поэтому в интерфейсе использованы максимально лаконично размещенные поля и кнопки(рисунки 1-2). Это во многом облегчает работу пользователя.





Рисунки 1-2. Вид окна пользователя клиента и сервера

**Заключение**

За время прохождения практики мне удалось закрепить и конкретизировать результаты теоретического обучения, приобрести умения и навыки практической работы по избранной специальности.

Практика в данной организации позволила развить навыки в таких сферах, как электроника, программирование, информационная безопасность, а также дала фундаментальные знания в изучаемых мной областях. Результаты исследований по теме разработки безопасного клиент-серверного приложения были включены в дипломный проект.

|  |  |
| --- | --- |
| Студент | Д.А. Данилин |
| Руководитель практики от организации, заместитель начальника отдела компьютерно-технических экспертиз управления компьютерно-технических экспертиз и экспертиз радиоэлектронных устройств главного управления технических экспертиз центрального аппарата Государственного комитета судебных экспертиз Республики Беларусь | А.А. Шаховец |