Министерство образования Республики Беларусь

Белорусский государственный университет

Факультет радиофизики и компьютерных технологий

Кафедра информатики и компьютерных систем

Отчет о производственной преддипломной практике

Данилин Даниила Алексеевича

студента 4 курса,

специальность

1-98 01 01 «Компьютерная безопасность»

Руководитель практики от организации:

Заместитель начальника управления технических экспертиз управления Государственного комитета судебных экспертиз Шаховец А. А.

Минск 2022

**Место прохождения практики:** управление технических экспертиз управления Государственного комитета судебных экспертиз

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

**Цель практики:** изучение методов, применяемых при проведении компьютерно-технических экспертиз.

**Задачи на практику:**

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

2. Изучение особенностей копирования информации из памяти компьютерной техники и мобильных устройств;

3. Использование современных методов восстановления удалённой информации;

4. Подготовка и оформление результатов проведения экспертизы (заключения эксперта);

5. 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.

С помощью 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 копирование информации, однако их методы и методы дальнейшего исследования имеют различия.

**Описание 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) внесении 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. В случае исследования мобильных устройств сделать побитовую копию не всегда представляется возможным в виду разнообразия устройств, операционных систем и их версий, а предлагаемые компаниями способы безопасности не всегда позволяют осуществить полную копию данных. Тогда в качестве альтернативы используется копия файловой системы или резервная копия. Копия файловой системы включает в себя копирование каталогов, однако в отличии от побитовой копии, не всегда будет возможно восстановление удаленной информации. С помощью резервной копии можно извлечь минимум исследуемой информации и, как правило, без возможности восстановления удалённых данных. Однако, при невозможности использовании других методов копирования информации, резервная копия все же будет основой для последующего анализа извлеченной информации. 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, проработки основных разделов пояснительной записки по теме дипломного проекта, а также разработка клиент-серверного приложения.

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

Также 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.

**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 компьютерной сфере, а также дала фундаментальные знания в этой области.

Результаты исследований по теме разработки безопасного клиент-серверного приложения были включены в дипломный проект.

Студент Д.А. Данилин

.04.2022

Руководитель практики

от БГУ, старший преподаватель Ю. А. Бондаренко

.04.2022

СОГЛАСОВАНО

Руководитель практики  
от организации А.А. Шаховец

.04.2022