**Тема**

Разработка программного модуля для защиты информации криптографическими и нетрадиционными методами при ее передачи.

**Структура**

* титульный лист;
* содержание;
* введение;
* основная часть, состоящая из 3-х глав;
* заключение;
* список использованных источников;
* приложения.
* требования безопасности
* защищаем передаваемую технологическую (техническую, служебную)
* важность реализации, решение вопросов
* почему именно мобильные устройства
* важность быстрой реакции

**Документ**: Базовая модель угроз безопасности персональных данных. 2008 г.

(в конце документа про стеганографию)

**Документы ЦБ:** Актуальные стандарты по защите информации.

**Введение**

Во***введении***

* обосновывается актуальность выбранной темы;
* формулируется проблема, которую дипломник должен решить в данной работе;
* определяются цели и задачи, решение которых необходимо для достижения данной цели;
* определяются объект и предмет исследования: объект - где проводится исследование (страна, город), на базе какой организации; предмет - что исследуется (например, социально-экономические, трудовые отношения по поводу... и пр.);
* даются композиционные особенности и краткое содержание теоретической и практической частей работы.

Рекомендуемый объем введения - 2-3 страницы.

**Основная часть**

***В первой главе*** ВКР рассматриваются теоретические вопросы по теме работы, дается обзор литературных источников (книг, журналов, монографий, газетных статей, материалов конференций и т.д.), освещаются законодательно-нормативные акты. Обзор литературы должен показать знание дипломником специальной литературы, его умение систематизировать источники, критически их рассматривать, выделять существенное, оценивать ранее сделанное другими исследователями, представлять современное состояние изученности темы.

В первой главе следует создать основу (базу) для последующих глав, которые будут конкретизировать теоретические положения работы. Объем первой главы дипломной работы составляет 18-20 страниц.

***Вторая глава*** носит аналитический характер. В ней приводится краткая характеристика объекта исследования в динамике, раскрываются особенности функционирования объекта. К числу их, как правило, относятся: общая характеристика объекта исследования (организации, структуры, законодательства, нормативных актов, практики деятельности и т.п., в зависимости от целей ВКР), целевые ориентиры и стратегии деятельности, результаты продуктово-рыночного анализа, организационная структура управления, система внешних и внутренних организационных, экономических и информационных связей, стратегическая позиция организации, анализ финансового состояния фирмы. Проводится общая оценка достижений и выявляются проблемы, имеющиеся в объекте исследования. В заключении второй главы дипломник определяет конкретную проблему, которую он разрабатывает (решает), пути и методы ее решения.

Объем второй главы примерно составляет 18-20 страниц.

***Третья глава***посвящена практическому решению поставленной проблемы. Эта часть ВКР должна носить проектный характер. Здесь разрабатываются новые подходы и направления деятельности, новые продукты и технологии, новые законодательные и нормативные акты и т.п. Вырабатывается система административных, экономических, социально-психологических мероприятий и процедур, необходимых для внедрения предлагаемых решений в практику деятельности. Мероприятия и пути их внедрения должны соответствовать логике теоретического и практико-ориентированного анализа, проведенного автором в первых главах, и полностью решать поставленные задачи.

В третьей главе излагаются и анализируются полученные результаты, дается прогнозная экономическая оценка предлагаемого варианта решения проблемы. Объем третьей главы работы 18-20 страниц.

**Заключение**

***В заключении*** последовательно излагаются теоретические и практические результаты и суждения, к которым пришел студент в результате исследования. Они должны быть краткими, четкими, дающими полное представление о содержании, значимости, обоснованности и эффективности работы. Результаты (выводы) исследования должны соответствовать поставленным цели и задачам.

Объем заключения 2-3 страницы.

***Список использованных источников***составляет одну из важных частей работы. Каждый включенный литературный источник должен иметь отражение в тексте выпускной квалификационной работы. Если автор делает ссылку на какие-либо заимствованные факты или цитирует работы других авторов, то он должен указать, откуда взяты приведенные материалы. Нельзя включать в библиографический список те работы, на которые нет ссылок в тексте работы, и которые фактически не были использованы.

***Приложения***призваны облегчить восприятие содержания работы и могут включать: дополнительные материалы, иллюстрации вспомогательного характера, анкеты, методики, документы, материалы, содержащие первичную информацию для анализа, таблицы статистических данных и др.

# Введение

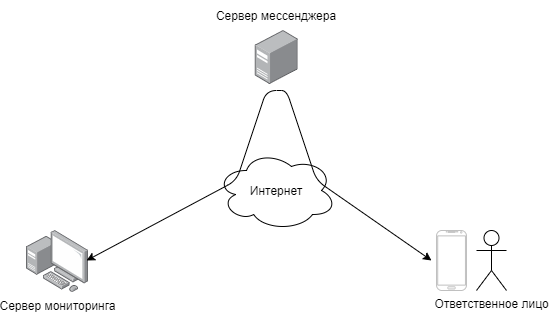
**Рассматриваемое предприятие:** ПАО Сбербанк (Кредитная организация)

Актуальность скрывать информацию даже внутри мессенджера обуславливается развивающейся киберпреступностью, атаками на сервера мессенджеров, внутренними утечками, организованной продажей клиентских данных, стремлением властей государств получить тотальную осведомленность о всем, чем общаются пользователи.

Необходимо разработать программный модуль для безопасной передачи технологической информации в мессенджере, который мы будем использовать в связи с необходимостью быстрого реагирования на инциденты, происходящие в системе, которую мы сопровождаем. Это позволит создать нам защищенный, стабильный канал без несения материальных затрат, внедрения кардинально новых систем и продуктов сторонних организаций.

Необходимость создания такого канала обусловлена риском перехвата этой технологической информации, что может нанести репетиционный ущерб предприятию, ухудшить отношение клиентов и как следствие повлиять на их отток и потерю финансовых оборотов как следствие.

Рассмотрим так же весь путь следования технологической информации (**Рассмотреть более детальную схему возможности потерять информацию, объяснить, почему для нас актуален только этот вариант**)



Очевидно, что информация может быть скомпрометирована как на этапе передачи до сервера мессенджера (в случае, если клиентом мессенджера не предусмотрено шифрование, что крайне редко встречается в наше время), так и на самом сервере. Здесь мы никак не можем повлиять на то, как поступит с нашей информацией непосредственно сам мессенджер. Скомпрометированная информация может быть передана третьим лица с целью получения выгоды и как следствие информация об инциденте на предприятии может принести репутационный ущерб кампании, которая не смогла сохранить в секрете информацию о внутренних проблема.

В случае использования своего шифрования уже до отправки сообщения в мессенджер риск того, что информация может быть скомпрометирована, сводится к качеству сокрытия информации, стойкости шифрования в частности.

Использование именно мессенджера как средства передачи позволяет без проблем установить программу на личный телефон сотрудника, который у него всегда под рукой. Это просто необходимо, так как зачастую в моменты критических событий требуется молниеносное реагирование на произошедший инцидент, пока он не повлиял на клиента.

Рассмотрим 2 ситуации.

Ситуация 1. В системе произошел критически важный инцидент, согласование решения которого возможно только с начальником отдела сопровождения. Из-за того, что важная информация не может быть передана безопасно на личный телефон, приходится использовать рабочий компьютер, доступ к которому этот самый начальник имеет далеко не всегда. Допустим, он отошел в магазин, за это время случился инцидент, о котором начальник узнает только когда вернется из магазина, за это время может произойти влияние на клиента, что понесет ущерб для всего банка.

Ситуация 2. Отличается она от ситуации 1 только тем, что у начальника на телефоне установлена программа, дающая ему связь с личного устройства. На произошедший инцидент он реагирует моментально, никакого влияния и ущерба не было допущено.