


Защита тайны связи в условиях новых цифровых угроз

Консманов А, 301-П

Научный руководитель: Лушников В.А



Введение: актуальность, цели, объекты и предметы исследования

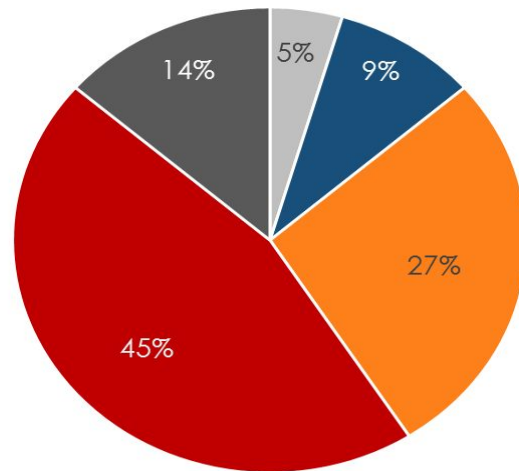
Актуальность:

- опережающие развитие средств атаки на тайну связи;
- быстрое появление новых математических и социальных алгоритмов атак;
- слабая информированность сотрудников государственных и даже крупных частных предприятий о данной проблеме;
- возможность изучения и анализа существующих средств защиты тайны связи и разработка новых.


Введение: актуальность, цели, объекты и предметы исследования

Актуальность:

Распределение видов атак,
применяемых
злоумышленниками
в 2016-2017 годах




- Атаки на веб-приложения
- Атаки типа "Отказ в обслуживании"
- Атаки методом социальной инженерии
- Атаки с использованием вредоносного ПО
- Атаки на инфраструктуру



Введение: актуальность, цели, объекты и предметы исследования

Цели:


- строгое определение понятий “тайна связи, цифровые угрозы”;
- правовые аспекты защиты тайны связи в РФ и в мире;
- анализ новых цифровых угроз;
- анализ существующих средств защиты частной цифровой переписки, выбор оптимальных для определенных задач;
- Опционально: разработка собственного ПО на основе существующих алгоритмов и/или с их модифицированием.



Введение: актуальность, цели, объекты и предметы исследования

Объекты и предметы исследования:

- Объекты: цифровые данные частных лиц в частных и организационных сетях, в первую очередь сама переписка и сведения об абонентах, то есть участниках переписки.;
- Предмет: изучение методов атак на частные данные, причины утечек этих данных, цели злоумышленников.



Понятие “цифровой угрозы”, новые цифровые угрозы

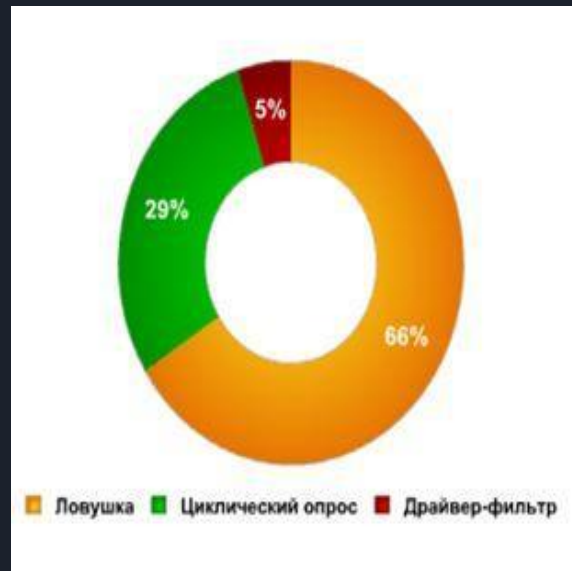
Цифровая угроза -- совокупность условий и факторов, создающих опасность нарушения информационной безопасности в контексте нарушения тайны связи; является случаем **угрозы информационной безопасности** -- угрозой конфиденциальности (неправомерный доступ к информации) и угрозой доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

Угрозы называются **новыми**, т.к. их бурное развитие и рост числа инцидентов произошли в последние 10-15 лет и сами угрозы постоянно меняются, увеличивается их количество.


Понятие “цифровой угрозы”, новые цифровые угрозы

Основные виды угроз в частном секторе:

- SpyWare. Отдельный класс вредоносного ПО, лишенный репликативных свойств вируса, предназначенный для мониторинга, сохранения и передачи злоумышленнику данных о работе ПО, пользовательской активности и самом пользователе посредством логирования нажатия клавиш или создания регулярных скриншотов экрана.
- Отдельным классом SpyWare считаются кейлоггеры, направленные на журналирование нажатых клавиш и работающие на низком уровне



Основные реализации кейлоггеров



Понятие “цифровой угрозы”, новые цифровые угрозы

Основные виды угроз в частном секторе:

Атаки на протоколы и средства связи, криптографические протоколы

- Man in the middle. MITM, атака посредника
- Подмена, спуфинг
- Повторное навязывание сообщения
- Параллельная атака
- Атака с использованием специально подобранных текстов
- Атака по известному сеансовому ключу
- Использование уязвимостей алгоритма или ошибок реализации

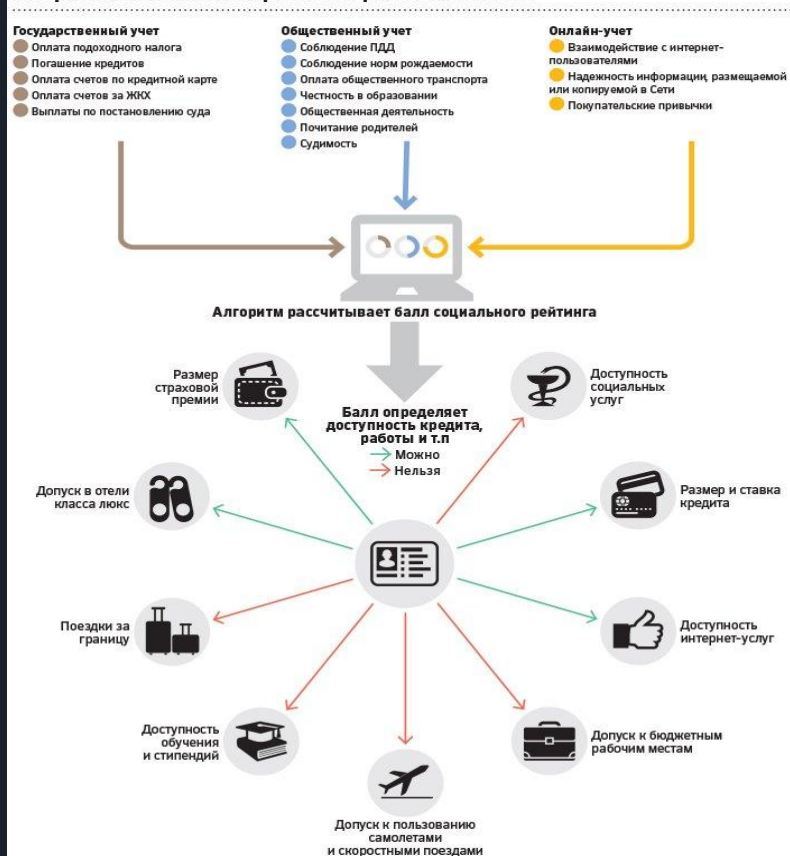
Понятие “цифровой угрозы”, новые цифровые угрозы


Государственный шпионаж за цифровой перепиской:

Китай проводит политику массовой слежки за гражданами по всей территории страны:

- “Золотой щит” -- система фильтрации содержимого интернета;
- Интернет-цензура;
- Система социального кредита -- система постоянного анализа поведения граждан в Интернете и в повседневной жизни, на схеме справа

Как работает Система социального рейтинга в Китае





Понятие “цифровой угрозы”, новые цифровые угрозы

Государственный шпионаж за цифровой перепиской:

США и ЕС.

- MAINWAY
- Tailored Access Operations
- Boundless Informant (см следующий слайд)
- PRISM
- NarusInsight
- Tempora
- MUSCULAR (см следующий слайд)
- Frenchelon
- Onyx

Понятие “цифровой угрозы”, новые цифровые угрозы

Boundless Informant u
MUSCULAR
на слайдах
SSO

TOP SECRET//SI//ORCON//NOFORN

Special Source Operations

Google, Yahoo!, AOL, Skype, paltalk.com, YouTube, Hotmail, Facebook, MSN

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

PRISM

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.

International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//NOFORN

Special Source Operations

Current Efforts - Google

PUBLIC INTERNET. GOOGLE CLOUD.


USER, MOBILE USER, GFE, DC, Gmail, Docs, Maps

GFE = Google Front End Server

SSL Added and removed here! :)

Traffic in clear text here.

TOP SECRET//SI//NOFORN



Понятие “цифровой угрозы”, новые цифровые угрозы

Государственный шпионаж за цифровой перепиской:

Россия

- СОРМ (1,2,3) -- система прослушивания телефонных коммуникаций, протоколирования обращений к сети Интернет, обеспечения сбора и долгосрочного хранения данных, получаемых от операторов связи, АТС, провайдеров интернет.
- Пакет Яровой-Озерового, направленный на постоянный анализ и хранение массивов Big Data со звонками и используемым интернет-трафиком

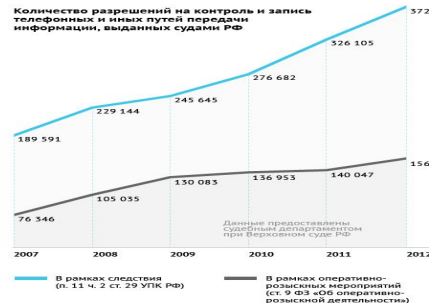
Понятие “цифровой угрозы”, новые цифровые угрозы

Принцип работы СОПМ

Прослушка телефонных переговоров и перехват трафика

Кто и как следит за разговорами в России

Количество разрешений на контроль и запись телефонных и иных путей передачи информации, выданных судами РФ



Процедура установки прослушки

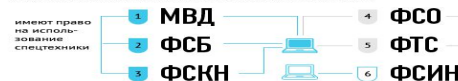
ФЕДЕРАЛЬНЫЙ ЗАКОН №404 (2010) РАЗРЕШАЕТ УСТАНОВКУ ПРОСЛУШКИ ПО РАЗРЕШЕНИЮ СУДА И ПРИ НАЛИЧИИ ИНФОРМАЦИИ:

- о признаках противоправного деяния, по которому производство предварительного следствия обязательно, или лица, таковое деяние подготавливающих
- о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической или экологической безопасности РФ

ПРОСЛУШИВАТЬ РАЗРЕШЕНО ТОЛЬКО ЛИЦ, ПОДОЗРЕВАЕМЫХ ИЛИ ОБВИНЯЕМЫХ В СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ (СРЕДНЕЙ ТЯЖЕСТИ, ТЯЖКИХ ИЛИ ОСОБО ТЯЖКИХ), ЛИБО ЛИЦ, КОТОРЫЕ МОГУТ РАСПОЛАГАТЬ СВЕДЕИЯМИ ОБ УКАЗАННЫХ ПРЕСТУПЛЕНИЯХ

С разрешения суда прослушка и перехват информации могут быть официально установлены:

В РАМКАХ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ:



- 1 – Министерство внутренних дел
- 2 – Федеральная служба безопасности
- 3 – Федеральная служба по контролю за оборотом наркотиков

- 4 – Федеральная служба охраны
- 5 – Федеральная таможенная служба
- 6 – Федеральная служба исполнения наказаний

Аппаратура

ДЛЯ ПЕРЕХВАТА ИНФОРМАЦИИ ИСПОЛЬЗУЮТСЯ УСТРОЙСТВА СОПМ (СИСТЕМА ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ)

Портативный СОПМ представляет собой ноутбук со специальным блоком, который можно подключать напрямую к узлам связи и оперативно перехватывать разговоры и трафик.

Вся аппаратура, кроме портативного СОПМ, подключается к коммуникационной сети

УСТАНОВКА АППАРАТУРЫ СОПМ ЯВЛЯЕТСЯ ОБЯЗАТЕЛЬНЫМ ТРЕБОВАНИЕМ К ОПЕРАТОРАМ СВЯЗИ

СОПМ-1

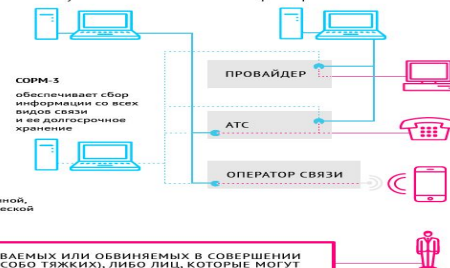
отвечает за прослушку телефонных линий, включая мобильную связь и VoIP

СОПМ-2

перехватывает интернет-трафик и телефонные переговоры

СОПМ-3

обеспечивает сбор информации со всех видов связи и ее долговременное хранение



В РАМКАХ СЛЕДСТВЕННЫХ МЕРОПРИЯТИЙ:

Органы следствия

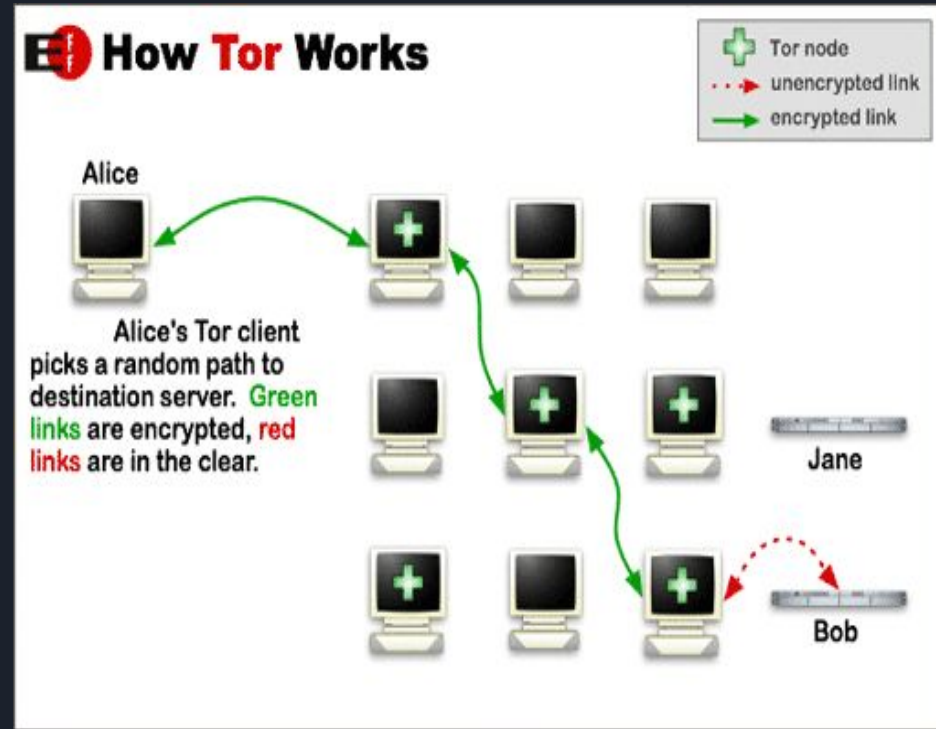
Кроме этого, прослушка может быть установлена:

- Службой внешней разведки (в рамках компетенции)
- ФСИН – в рамках контроля за находящимися под домашним арестом

Защита личной переписки

Обзор существующего ПО для защиты переписки и его анализ:

- TOR, луковые сети (см справа);
- I2P, чесночная маршрутизация;
- JonDo;
- GNU FreeNet;



Защита личной переписки

Обзор существующего ПО для защиты переписки и его анализ:

- Ремейлеры;
- Стеганография. Справа представлен fusion-метод передачи изображения: фото кота вшито в фото дерева



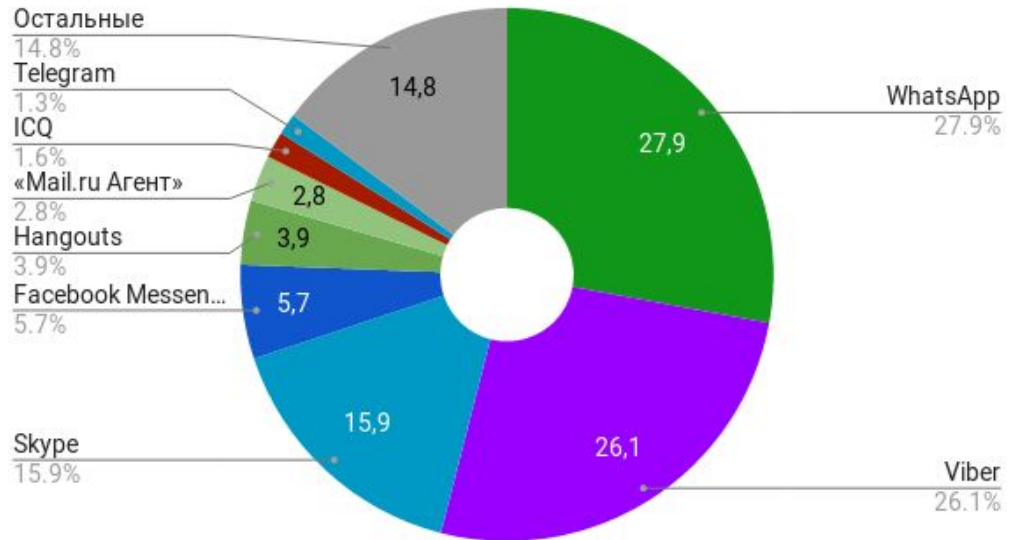
Защита личной переписки

Обзор существующего ПО для защиты переписки и его анализ:

Мессенджеры:

- Viber
- WhatsApp
- Telegram

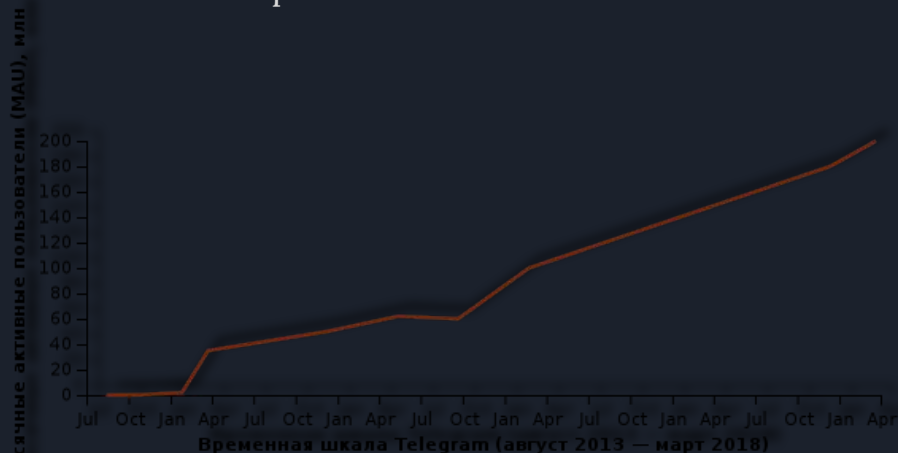
Самые популярные в России мессенджеры. Доля аудитории, %



Защита личной переписки

Обзор существующего ПО для защиты переписки и его анализ:

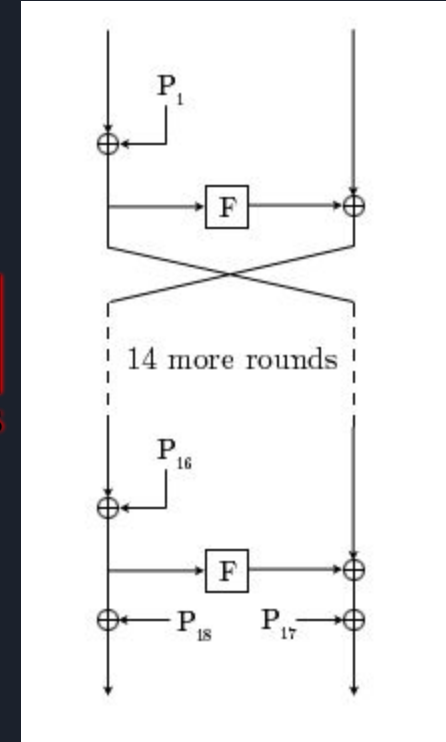
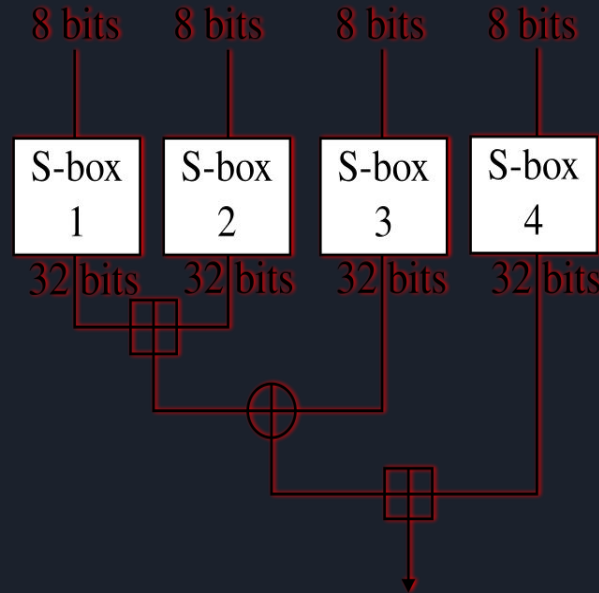
Технологии Telegram: MTProto, сквозное шифрование, политика неразглашения, секретные чаты, конфликт с РКН



Защита личной переписки

Разработка собственного ПО:

- Выбор алгоритма (Blowfish, симметричное блочное шифрование);
- Описание алгоритма (Сеть Фейстеля, XOR);
- Выбор средств реализации (C#.Net 4.5);
- Успех реализации;
- Криптостойкость, сильные и слабые стороны



Функция $F(x)$ в Blowfish и Сеть Фейстеля при зашифровании

Заключение:

- Дано четкое определение понятиям <<тайна связи, личная переписка, нарушение тайны связи, цифровая угроза>>;
- Рассмотрены существующие законодательные нормы и тенденции, мировая практика в области защиты тайны связи;
- Определены основные существующие угрозы для сохранения тайны переписки, проведен их детальный анализ;
- Проведен детальный анализ существующих программных средств для сохранения цифровой тайны переписки, выбраны оптимальные продукты для различных ситуаций, на основе существующих алгоритмов разработан свой собственный программный продукт, позволяющий проводить эффективное и устойчивое шифрование данных.



Спасибо
за
внимание

