Security Engineering: часть 11. Электронная и информационная война, а также Безопасность телекоммуникаций

Published: 25.06.2026 10:42 | Updated: 25.06.2026 15:58

Электронная, информационная война и безопасность телекоммуникаций: Фундаментальные принципы и угрозы

Электронная и информационная война (Основы, Связь и SIGINT)

> «Всякая война основана на обмане... выманивайте противника приманкой... притворяйтесь беспорядочным и сокрушайте его». — Сунь-цзы, «Искусство войны».
> «Сила и обман — две главные добродетели на войне». — Томас Гоббс.

На протяжении десятилетий электронная война (e-war) оставалась отдельной дисциплиной, параллельной компьютерной безопасности, несмотря на использование общих технологий, таких как криптография. Однако сегодня эти области сливаются в новую дисциплину — информационную войну (i-war). Принятие Пентагоном термина «информационная война» в конце XX века закрепило ее важность, а кибератаки, подобные российским DDoS-атакам на Эстонию в 2007 году, вывели эти угрозы на уровень государственной политики.

Электронная война предоставляет уникальные уроки для инженеров по безопасности. Борьба за контроль над электромагнитным спектром потребовала миллиардов долларов и породила стратегии обмана невероятной глубины и тонкости. Это единственная область электронной безопасности, которая пережила длительную эволюцию атак и защиты с участием способных и мотивированных противников. Кроме того, именно электронная война является главным учителем в области атак типа «отказ в обслуживании» (DoS).
В то время как классическая компьютерная безопасность фокусируется на конфиденциальности, целостности и доступности, электронная война переворачивает эти приоритеты:

1. **Отказ в обслуживании** (глушение, мимикрия, физическая атака).
2. **Обман** (направленный на автоматические системы или людей).
3. **Эксплуатация** (перехват и получение любой оперативной информации из электронных систем противника).

Базовые концепции электронной войны

Целью электронной войны является контроль над электромагнитным спектром. Она традиционно делится на три компонента:

- **Электронная атака (EA):** Глушение коммуникаций или радаров противника, а также нарушение работы его оборудования с помощью мощных микроволновых излучений.
- **Электронная защита (EP):** Проектирование систем, устойчивых к глушению, защита оборудования от атак мощными микроволновками и уничтожение вражеских глушителей с помощью противорадиолокационных ракет.
- **Электронная поддержка (ES):** Сбор разведданных и распознавание угроз, позволяющее эффективно осуществлять атаку и защиту. Это включает поиск, идентификацию и локализацию источников преднамеренного и непреднамеренного электромагнитного излучения. Традиционная криптография (защита коммуникаций или COMSEC) является лишь малой частью электронной защиты.

Системы связи и угрозы

Военные коммуникации исторически эволюционировали от физических курьеров до телеграфа, телефона и современных радиосетей. Без ситуационной осведомленности и средств управления войсками командующий неэффективен.
Типы трафика и угрозы:

- **Стратегические сети** (между штабами и политическим руководством): Главная угроза — взлом шифров, саботаж, кража ключей или внедрение ложных сообщений. Защита включает не только шифрование, но и защиту от анализа трафика (например, сквозное шифрование каналов). Вторичная угроза — физическое уничтожение кабелей или ретрансляционных станций.
- **Сети для скрытых активов** (агенты в поле): Помимо криптозащиты, критически важна **локационная безопасность**. Агент должен минимизировать риск обнаружения средствами радиопеленгации и анализа трафика. Если используется публичная сеть, усилия агента сосредоточены на маскировке факта коммуникации.
- **Тактические коммуникации** (между штабом и подразделением в поле): Уязвимы к глушению и внедрению обманных сообщений. Например, существует оборудование, позволяющее перехватывать голосовые команды вражеского авиадиспетчера, разрезать их на фонемы и склеивать для передачи ложных команд пилотам.
- **Командные и телеметрические сети** (сигналы от самолета к только что запущенной ракете): Должны быть защищены от глушения и модификации. Желательно, чтобы они были скрытными (не memicu предупреждающие приемники противника), что конфликтует с необходимостью высокой мощности для преодоления защитного глушения. Решение — адаптивные системы, начинающие работу в режиме с низкой вероятностью перехвата (LPI) и повышающие мощность только при обнаружении глушения.

Сигнальная разведка (SIGINT)

Прежде чем атаковать сеть, ее необходимо картографировать. SIGINT делится на **COMINT** (разведка коммуникаций — контент и метаданные) и **ELINT** (электронная разведка — распознавание вражеских радаров и некоммуникационных источников).

Техники SIGINT:

- **RF-фингерпринтинг (Radio Frequency Fingerprinting):** Идентификация конкретного оборудования по уникальным характеристикам сигнала. Сюда входят непреднамеренная частотная модуляция, форма переходного процесса при включении передатчика, точная центральная частота и гармоники усилителя. Эта технология, ранее секретная, была рассекречена в 1990-х для борьбы с клонированием сотовых телефонов.
- **Радиопеленгация (RDF):** Исторически использовала направленные антенны на двух станциях. Современные системы используют **TDOA (Time Difference of Arrival)** — сравнение фаз сигналов, принятых на двух разнесенных пунктах, что позволяет быстро, точно и автоматически локализовать источник.
- **Анализ трафика:** Изучение объема и паттернов сообщений. Даже зашифрованный трафик выдает информацию. Классический пример — «снежный ком» (snowball search). Если подозреваемый «Алиса» находится под наблюдением, аналитики фиксируют всех, кому она звонит, и всех, кто звонит ей. Отсеяв «белые списки» (банки, врачи), аналитики рекурсивно применяют этот метод к оставшимся контактам. В результате формируется массив (снежный ком) из тысяч контактов, в котором выявляются скрытые связи и узлы сети.

Атаки на коммуникации

Атака может включать физическое уничтожение (жесткое убийствие — hard kill) или глушение/обман (мягкое убийство — soft kill).

Глушение и обман:

- **Шумовое глушение (Barrage jamming):** Генерация мощного шума в диапазоне частот противника. Контрмера — использование приемника с защитной полосой (guard band receiver) на соседней частоте; при обнаружении шума полезный сигнал блокируется.
- **Обманные передатчики (Repeater/Transponder):** Перехват сигнала противника, его модификация и отправка обратно.

- **Голосовой морфинг:** В воздушных боях и конфликтах (например, в войнах в Корее, Вьетнаме и на Ближнем Востоке) системы идентификации «свой-чужой» (IFF) и голосовые коммуникации подвергались атакам. Перехваченные голосовые команды разрезались на фонемы и склеивались для создания убедительных ложных приказов.

Методы защиты коммуникаций

Для защиты от перехвата и глушения используются специфические технологии.
Направленные и скрытные каналы:

- Оптические линии (инфракрасные лазеры) или СВЧ-линии с узконаправленными антеннами и экстремально высокими частотами.
- **LPI (Low-Probability-of-Intercept)** и **LPPF (Low-Probability-of-Position-Fix)** — технологии с низкой вероятностью перехвата и пеленгации.

Спектральное расширение (Spread Spectrum):
Изначально разработанное для военных целей, эта технология легла в основу современных коммерческих стандартов (CDMA, GPS, WiFi).

1. **Скачкообразная перестройка частоты (Frequency Hopping):** Передатчик быстро переключается между частотами по псевдослучайному алгоритму, известному только легитимным сторонам.
   -- Исторический факт: Эта технология была изобретена в 1940 году актрисой **Хеди Ламарр** и композитором **Джорджем Антейлом**. Они предложили систему управления торпедами, где передатчик и приемник синхронно перестраивали частоты, используя перфорированную ленту, аналогичную той, что использовалась в механических пианино. Патент был передан ВМС США, но реализован только десятилетия спустя.
   -- Защита: Если противник не знает последовательности скачков, ему приходится глушить весь диапазон, что требует колоссальной мощности.
2. **Прямая последовательность (DSSS - Direct Sequence Spread Spectrum):** Информационный сигнал умножается на псевдослучайную последовательность с гораздо более высокой скоростью (чиповой). Это «размазывает» сигнал по широкой полосе частот, делая его похожим на фоновый шум. На приемнике сигнал восстанавливается путем корреляции с той же последовательностью.
3. **Импульсная передача (Burst Communications / Time-hop):** Данные сжимаются и передаются короткими импульсами в непредсказуемое время. Если коэффициент заполнения низок, сканирующий приемник противника может просто пропустить передачу.

4. **Метеорное рассеяние (Meteor Scatter):** Использование ионизационных следов от микрометеоритов в атмосфере для создания временных каналов связи на расстояния 500–1500 км. Материнская станция передает непрерывно, а дочерняя станция, попав в зону «видимости» следа, быстро отправляет пакеты данных. Применяется для связи с удаленными радарами раннего предупреждения и в гражданских целях для мониторинга осадков в развивающихся странах.

Никки Хагер (Nicky Hager) и система Echelon

Журналист Никки Хагер, который в своей книге «Secret Power» подробно описал работу глобальной системы перехвата Echelon, управляемой странами UKUSA (США, Британия и др.). Он описал, как «словари» (dictionaries) автоматически фильтруют перехваченный трафик по ключевым словам, и как разведывательные сообщества используют эти данные для экономического и политического шпионажа.

Наблюдение и целеуказание

Хотя некоторые сенсорные системы используют пассивную пеленгацию, основными методами обнаружения вражеских целей и наведения на них оружия являются сонар, радар и инфракрасные системы. Если сонар зародился в Первую мировую войну, то радар стал ключевым фактором во Второй мировой. Именно в области радиолокации были в наибольшей степени развиты искусства атаки (глушения) и защиты (электронной защиты).

Типы радаров

Используется широкий спектр систем, включая поисковые радары, радары управления огнем, радары следования за рельефом, контрбатарейные радары и метеорологические радары. У каждого из них свои характеристики сигналов: например, радары с низкой радиочастотой и низкой частотой повторения импульсов (PRF) лучше подходят для поиска, тогда как высокочастотные системы с высоким PRF эффективнее для сопровождения целей.

Техники глушения

Электронная атака может быть пассивной или активной.

- **Дипольные отражатели (Chaff):** Классическая пассивная мера. Тонкие полоски проводящей фольги, нарезанные под половину длины волны целевого сигнала, сбрасываются с самолета для создания ложных эхо-сигналов. Во время Второй мировой войны союзники сбрасывали до 2000 тонн дипольных отражателей в день, чтобы ослепить немецкую ПВО. Главной контрмерой против них стало использование доплеровских радаров, так как облако фольги быстро теряет скорость и легко отделяется от движущейся цели.
- **Ложные цели (Decoys):** Могут представлять собой небольшие устройства с активными ретрансляторами или крупные платформы, просто отражающие радиосигналы. Они применяются для отвлечения внимания систем ПВО или ракет с радиолокационным наведением.
- **Активные методы глушения:**
  -- Шумовое глушение (Barrage/Noise jamming): Генерация мощного шума в диапазоне частот радара. Контрмерой является использование радарами сжатия импульсов или доплеровской фильтрации.
  -- Глушение с инверсией усиления (Inverse gain jamming): Радар излучает сигнал не только через основной луч, но и через боковые лепестки диаграммы направленности. Глушитель анализирует эти боковые лепестки и транслирует искаженный сигнал обратно, заставляя радар «видеть» цель там, где ее нет, или искажая данные о дальности и азимуте.
  -- Глушение с перекрытием (Cover jamming): Создание мощного сигнала, который перекрывает слабый эхо-сигнал от цели, делая ее невидимой на фоне помехи.

Современные радары и контрмеры

Для борьбы с глушением радары эволюционируют:

- **Сжатие импульсов (Pulse compression):** Позволяет передавать длинные, но сложные импульсы (например, с фазовой модуляцией), которые при обработке сжимаются в узкий пик. Это дает высокое разрешение и защиту от простых шумовых помех.
- **Импульсно-доплеровские радары (Pulsed Doppler):** Критически важны для выделения движущихся целей на фоне земных помех (clutter). Они анализируют сдвиг частоты, вызванный эффектом Доплера.

- **Моноимпульсные радары (Monopulse):** Используют несколько диаграмм направленности одновременно для высокоточного определения угловых координат цели за один импульс, что делает их крайне устойчивыми к угловому глушению.

Другие сенсоры и мультисенсорные проблемы

Инфракрасные (тепловые) сенсоры также широко применяются для наведения ракет. Контрмерой против них служат **тепловые ловушки (flares)** — пиротехнические устройства, создающие более яркий источник ИК-излучения, чем двигатель самолета. Однако современные ИК-головки самонаведения учатся отличать цели от ловушек по профилю излучения.
Современные платформы используют **слияние данных (multisensor data fusion)**, комбинируя информацию от радаров, ИК-камер, оптических систем и даже данных от пилотов. Однако интеграция этих систем создает новые уязвимости: если один сенсор выходит из строя или подвергается целенаправленной атаке, это может дезориентировать всю систему управления огнем.

Системы IFF («Свой-чужой»)

Идентификация «свой-чужой» (Identify-Friend-or-Foe, IFF) является критической и одновременно крайне спорной областью. Ошибки IFF приводят к инцидентам «дружественного огня» (blue-on-blue), которые наносят тяжелый моральный и политический ущерб.
История IFF уходит корнями в античность, но техническая эра началась во Вторую мировую войну, когда скорость самолетов сделала визуальную идентификацию невозможной. Ранние системы просто транслировали серийный номер или «код дня», что делало их уязвимыми для спуфинга (имитации). Позже были внедрены криптографические системы challenge-response.
Современные системы, такие как **Mark XII**, используют криптографические блоки (предшественники DES) для шифрования 32-битного запроса (challenge) и 4-битного ответа. Чтобы предотвратить атаки типа «MIG-in-the-middle» (ретрансляцию запросов и ответов), антенна радара, генерирующего запрос, является узконаправленной (обычно это радар управления огнем), в то время как приемник ответа работает в широком секторе.
Проблемы и организационные барьеры:
Несмотря на технологический прогресс, инциденты «синих против синих» продолжаются. В войне в заливе и в Ираке они случались из-за несовместимости оборудования разных стран коалиции, задержек в обновлении баз данных и

человеческого фактора. Попытки создать единую систему IFF для НАТО часто буксуют из-за политических трений: страны не хотят раскрывать свои криптографические ключи союзникам, опасаясь утечек. В результате коалиционные силы часто вынуждены полагаться на процедурные меры (например, «коридоры» для полетов), которые менее надежны, чем технические средства.

Самодельные взрывные устройства (IED)

Самодельные взрывные устройства (Improvised Explosive Devices, IED) стали «подписным оружием» повстанцев в Ираке и Афганистане. С 2003 года произошло более 80 000 атак с их использованием.
Изначально многие IED детонировались по радиосигналу (с использованием брелоков, мобильных телефонов). В ответ коалиционные силы развернули масштабную программу радиоэлектронной борьбы (РЭБ), установив на технику и базы мощные глушители, подавляющие частоты сотовой связи и радиоуправления.
Однако противник быстро адаптировался. Это классический пример **асимметричного конфликта**:

1. Переход на **проводные детонаторы** (command wires), которые невозможно заглушить радиоэлектронными средствами.
2. Использование **пассивных инфракрасных датчиков** и датчиков давления (жертва сама наезжает на мину или проходит мимо нее).
3. Тактика «мягкого отказа»: использование таймеров или замыкание цепи только при специфических условиях (например, при определенном уровне вибрации).

Опыт Ирака показал, что радиоэлектронная борьба эффективна только до тех пор, пока противник привязан к радиоэлектронике. Как только порог входа снижается (провод, датчик давления), технологическое превосходство нивелируется, и требуются совершенно иные методы защиты (бронирование, траление, разведка).

Конкретная статистика по IED (Самодельным взрывным устройствам) в Ираке

С 2003 года произошло более 81 000 атак с использованием IED. Пентагон потратил более $1 млрд на разработку глушилок. В результате радиоэлектронной борьбы процент радиоуправляемых IED упал с 70% до 10%, что заставило террористов перейти на проводные детонаторы и пассивные ИК-датчики.

Оружие направленной энергии

Оружие направленной энергии (Directed Energy Weapons) включает в себя лазеры, микроволновые пушки и генераторы электромагнитного импульса (ЭМИ).

- **Электромагнитный импульс (ЭМИ / EMP):** При ядерном взрыве в атмосфере или космосе гамма-излучение выбивает электроны из молекул воздуха, создавая колоссальные токи. ЭМИ способен вывести из строя всю электронную инфраструктуру на континенте. Именно из-за этой угрозы критически важные военные системы (командные пункты, шахты МБР) экранируются по стандартам TEMPEST и защищаются от ЭМИ.
- **СВЧ-оружие (High-Energy RF / HERF):** Существуют устройства, способные генерировать направленные микроволновые импульсы для «поджаривания» электроники на расстоянии (например, для уничтожения двигателей ракет или отключения компьютеров в бункере).
- **Террористическая угроза:** Существуют опасения, что террористы могут использовать компактные генераторы ЭМИ или СВЧ-пушки для атак на финансовые центры. Однако физика требует огромных источников питания и антенн, что делает создание «чемоданной» бомбы ЭМИ крайне маловероятным. Реальная угроза ЭМИ исходит в первую очередь от государственных структур (ядерное оружие), а не от террористов-одиночек.

Информационная война

Термин «информационная война» (Information Warfare, I-war) стал популярным после операции «Буря в пустыне», когда стало ясно, что доминирование в сборе и обработке информации так же важно, как и огневая мощь.

Определения и Доктрины

Как и в классической электронной войне, цели информационной войны можно разделить на три категории:

1. **Отказ в обслуживании (Denial):** Уничтожение или блокировка каналов связи, баз данных или систем управления противника.
2. **Обман (Deception):** Внедрение ложной информации в системы противника (например, через взлом баз данных или фишинг).
3. **Эксплуатация (Exploitation):** Кража данных (шпионаж, перехват трафика).

Доктринально информационная война опирается на древние принципы. Сунь-цзы писал: «Всякая война основана на обмане». Томас Гоббс называл силу и обман «двумя главными добродетелями на войне». В современном Пентагоне концепция I-war рассматривается как способ достичь «информационного превосходства», позволяющего вести операции без эффективного противодействия.

Уроки из электронной войны

Информационная война во многом наследует принципы электронной:

- **Фильтры защитных полос (Guard band receivers):** В e-war используется для обнаружения шумового глушения. В I-war аналогом является создание «ловушек» (honey traps) или систем мониторинга аномалий в базах данных, чтобы отличить легитимный трафик от атаки.
- **Ложные срабатывания (False alarms):** В e-war чрезмерное количество ложных целей снижает бдительность операторов. В I-war DDoS-атаки или спам-рассылки могут использоваться не столько для прямого ущерба, сколько для «утомления» систем защиты и персонала, чтобы скрыть истинную цель атаки.
- **Мягкое и жесткое уничтожение (Soft kill vs Hard kill):** В e-war «мягкое убийство» (глушение) обратимо, а «жесткое» (уничтожение антенны) — нет. В I-war «мягким убийством» может быть изменение записей в базе данных или внедрение логической бомбы, а «жестким» — физическое уничтожение серверной.

Отличия между E-war и I-war

Несмотря на сходство, между классической электронной войной и современной информационной войной есть фундаментальные различия, связанные с природой сетей:

1. **Асимметричный и партизанский конфликт:** В e-war (например, в воздушном бою) обычно сталкиваются технологически сопоставимые противники. В I-war доминируют асимметричные конфликты. Хакеры-одиночки или небольшие группы (скрипт-кидди, хактивисты) могут нанести ущерб, сопоставимый с действиями целых армий, используя дешевые инструменты против дорогой инфраструктуры.
2. **Открытость среды:** Электронная война ведется в контролируемом электромагнитном спектре. Информационная война ведется в открытом Интернете. Атакующий может находиться в любой точке мира, использовать анонимные прокси и ботнеты. Защита периметра здесь практически невозможна.
3. **Отсутствие четких границ:** В e-war есть четкое разделение на «свои» и «чужие» радиочастоты. В I-war трафик противника может быть неотличим от трафика мирных пользователей (например, при DDoS-атаках, использующих подчиненные компьютеры обычных граждан).
4. **Человеческий фактор:** В e-war основные цели — технические системы (радары, рации). В I-war главной целью и одновременно самым уязвимым звеном является **человек**. Социальная инженерия, фишинг и психологические операции (влияние на общественное мнение через соцсети) играют в I-war гораздо большую роль, чем в классической e-war.

Телекоммуникации как полигон для инженеров по безопасности

Защита телекоммуникационных систем представляет собой важнейший пример (case study) для инженеров по безопасности. Во-первых, многие распределенные системы в той или иной форме опираются на стационарные или мобильные телефонные сети, и способы, которыми эти зависимости проявляются, часто неочевидны. Надежность этих сетей неуклонно снижается. Если раньше телефонные станции (POTS) оснащались резервными дизель-генераторами, способными работать неделями, то современные сотовые вышки работают от аккумуляторов, которых хватает максимум на 48 часов. Более того, сами

электрические компании теперь полагаются на мобильные телефоны для координации ремонтных бригад, создавая уязвимые циклические зависимости.
Во-вторых, история уязвимостей телекоммуникаций поучительна. Первые атаки совершались энтузиастами («фриками») ради бесплатных звонков; затем уязвимости начали эксплуатировать мошенники, чтобы уклоняться от прослушки, с появлением платных номеров возникли масштабы для крупного мошенничества, а после либерализации рынков сами телефонные компании начали атаковать клиентов друг друга (и даже самих себя). Этот же паттерн повторяется и сегодня в интернете, только с многократно ускоренной историей. Многие политические вопросы, такие как прослушка, уже разыгрались на телефонных сетях и теперь воспроизводятся в IP-среде.
Наконец, телеком-индустрия учит нас тому, как технические меры защиты взаимодействуют с бизнес-моделями. Переход на IP-сети и конвергенция сервисов создают новые, непредвиденные уязвимости.

Телефонный фрикинг (Phone Phreaking)

Аборигены использовали оптические телеграфы (семафоры и гелиографы) еще в классические времена, но с изобретением электрического телеграфа в середине XIX века начались и первые злоупотребления. Например, букмекеры подкупали операторов или использовали подзорные трубы, чтобы перехватывать результаты скачек до того, как они достигнут официальных телеграфных линий. Законы, запрещавшие такие махинации, оказывались неэффективными.
С появлением телефона история повторилась. Ниже мы рассмотрим основные векторы атак на традиционные телефонные сети.

Атаки на системы тарификации (Attacks on Metering)

Ранние системы тарификации были уязвимы до смешного. В 1950-х годах, когда оператору нужно было услышать звук падающих монет в таксофоне, чтобы засчитать оплату, некоторые люди научились бить по монетоприемнику куском металла, издавая звук, который система распознавала как номинал монеты. Позже, когда оператор сам соединял междугородние звонки и спрашивал номер абонента для выставления счета, мошенники просто называли чужой номер. Чтобы защититься от этого, операторы начали перезванивать на указанный номер для подтверждения. В ответ фрики придумали трюк с таксофонами: они набирали номер, дожидались, пока их соединят, бросали трубку и тут же набирали номер снова. При повторном наборе сигнал «вызов из таксофона» не передавался оператору, и мошенник мог говорить по чужому счету.
Другим методом стало «паразитное подключение» (clip-on fraud).

Злоумышленники физически подключали свой телефон к чужой линии, чтобы воровать сервис. В 1970-х и 80-х годах это было популярно среди иностранных студентов, которые таким образом звонили домой, а счета приходили ничего не подозревающим домовладельцам.

Атаки на сигнализацию (Attacks on Signaling)

До 1980-х годов телефонные сети использовали внутриканальную сигнализацию (in-band signaling), когда управляющие тоны передавались по той же линии, что и голос. Это открыло путь к знаменитым «синим ящикам» (blue boxes).
Фрики обнаружили, что если подать в линию тон частотой 2600 Гц, это имитирует сигнал «отбой» (clear down), разрывая соединение на стороне телефонной станции, но оставляя магистраль (trunk) захваченной на стороне пользователя. После этого с помощью «синего ящика» можно было генерировать управляющие импульсы для набора любых междугородних или международных номеров бесплатно.
У телефонного фрикинга был и идеологический подтекст. В эпоху, когда телефонные компании воспринимались как безликие монополии, а контркультура 1960-х бросала им вызов, фрики считались своего рода героями. Однако с переходом на цифровые сети и выделенные каналы сигнализации (out-of-band) эти атаки стали историей, уступив место более изощренным методам.

Джо Энгресия (Joe Engresia) и «тотальный слух»

Джо Энгресия — глухой мальчик, который в 1960-х годах обнаружил, что может управлять телефонной сетью AT&T, потому что обладал абсолютным музыкальным слухом. Он мог на слух определять и воспроизводить тональные частоты (включая знаменитый тон 2600 Гц), используемые для маршрутизации междугородних звонков, просто свистя или используя генераторы тонов.

Атаки на коммутацию и конфигурацию (Attacks on Switching and Configuration)

С развитием цифровых АТС (PBX) и корпоративных сетей мишенью стали сами коммутаторы. Злоумышленники, получившие доступ к корпоративной АТС, могли использовать ее для совершения дорогостоящих междугородних звонков (dial-through fraud).
Особую проблему представляли инсайдеры. Владельцы или администраторы мелких АТС часто вступали в сговор с мошенниками, продавая доступ к своим

системам для маршрутизации нелегального трафика. В таких случаях защита сводилась не к криптографии, а к организационным мерам и мониторингу аномальных паттернов вызовов.

Незащищенные оконечные системы (Insecure End Systems)

Огромный пласт уязвимостей связан не с сетью, а с устройствами на стороне пользователя. Классическим примером является атака через автоответчики. Мошенники записывали на пленку номер платной линии, а затем звонили жертвам. Когда жертва брала трубку, мошенник «бросал» вызов, и автоответчик жертвы, пытаясь дозвониться до сброшенного номера, автоматически набирал записанный мошеннический платный номер.
Еще более масштабным стало мошенничество с платными номерами (premium rate scams). Злоумышленники создавали фиктивные сервисы, обещая бесплатные звонки или доступ к контенту, но перенаправлявшие вызовы на дорогие платные линии.
Одним из самых известных примеров стала «Молдавская афера». Порнографические сайты в США привлекали пользователей обещаниями бесплатного доступа, но при подключении модема происходило перенаправление на платные номера в Молдове. Пользователи получали счета на тысячи долларов за междугороднюю связь, даже не подозревая, что их модем физически соединился с другим государством.

Взаимодействие функций (Feature Interaction)

Телефонные сети предлагают множество дополнительных услуг, и их взаимодействие часто создает непредвиденные уязвимости.

- **Справочные службы:** Номера справочных служб (например, 118 118 в Великобритании) предназначены для получения номеров телефонов. Однако мошенники научились использовать их для совершения звонков или сокрытия своих следов. Например, супружеские изменники использовали справочные службы, чтобы скрыть факт звонка любовнице — в детализации звонков значился лишь безобидный номер справочной.
- **Переадресация вызова (Call forwarding):** Эта функция позволяет перенаправлять входящие звонки на другой номер. Злоумышленники использовали ее для обхода систем безопасности или для совершения мошеннических звонков, выдавая себя за других лиц, чьи номера были переадресованы на подконтрольные мошенникам линии.

- **Конференц-связь:** Функция объединения нескольких абонентов в один вызов также эксплуатировалась. Например, хулиганы или мошенники могли использовать конференц-связь, чтобы обойти ограничения на длительность звонков или скрыть истинного инициатора разговора, создавая сложные цепочки перенаправлений.

Эти примеры демонстрируют, как дополнительные функции, созданные для удобства, часто ломают базовые предположения о безопасности и тарификации, создавая новые векторы для атак.

Мобильные телефоны

С момента своего появления в качестве дорогой роскоши в начале 1980-х годов мобильные телефоны стали одним из величайших технологических успехов. К 2007 году в мире насчитывалось более миллиарда абонентов. Мобильные телефоны используются для самых разных целей: от покупки билетов на паром до получения банок с колой из торговых автоматов. Преступники также активно используют эти устройства: в провинции Катанга (ДРК) мобильные телефоны стали де-факто валютой, а похитители требуют выкуп, указывая номера для пополнения счета.

Клонирование мобильных телефонов

Первое поколение мобильных телефонов использовало аналоговые сигналы без какой-либо реальной аутентификации. handset (трубка) просто передавала свои серийные номера в открытом виде по радиоканалу. Злоумышленники создавали устройства для перехвата этих номеров. Основным потребителем таких краденых номеров были операции «call-sell» (нелегальная продажа междугородней связи), где мошенники торговали минутами, используя клонированные телефоны.
Позже появились «тумблеры» (tumblers) — телефоны, которые генерировали новый идентификатор для каждого звонка, что делало их практически не отслеживаемыми. В ответ индустрия внедрила системы обнаружения вторжений и RF-фингерпринтинг (радиочастотную дактилоскопию), которая идентифицирует конкретное устройство по уникальным искажениям сигнала, возникающим из-за производственных допусков в радиокомпонентах.

Механизмы безопасности GSM

Переход на цифровые стандарты, в частности GSM (Global System for Mobile Communications), принес с собой криптографическую аутентификацию. Персонализация абонента осуществляется с помощью SIM-карты.
Протокол аутентификации работает следующим образом:

1. Сеть отправляет случайный вызов (RAND).
2. SIM-карта вычисляет ответ (SRES), используя секретный ключ аутентификации (K_i), зашитый в карту и известный домашнему реестру местоположения (HLR).
3. Для вычисления используется односторонняя функция Comp128 (алгоритмы A3/A8).

Уязвимость Comp128: Оказалось, что этот алгоритм имеет «узкое горлышко» (narrow pipe). Злоумышленник, выступая в роли фальшивой базовой станции, может отправить SIM-карте около 150 000 специально подобранных вызовов и восстановить секретный ключ K_i. Это позволяло клонировать SIM-карты без физического доступа к ним.
Для защиты контента (разговоров) используется потоковый шифр A5. Однако и он был взломан (атака Флюрера-Мантина-Шамира и последующие атаки с использованием кэш-памяти), что позволило перехватывать и расшифровывать трафик.
Еще одной проблемой стали **IMSI-catchers** (перехватчики IMSI). Это фальшивые базовые станции, которые заставляют телефон зарегистрироваться у себя, выдавая себя за легитимную сеть. Это не только позволяет перехватывать звонки, но и нарушает конфиденциальность местоположения абонента.

Третье поколение мобильной связи (3GPP)

Стандарт 3G (UMTS) был разработан с учетом ошибок GSM. Используется блочный шифр Kasumi. Аутентификация стала двусторонней (сеть и телефон проверяют друг друга), а вычисления переносятся из SIM-карты в сеть (в VLR).
Здесь вновь всплыла проблема «бэкдоров». Правительства требовали механизмов перехвата трафика. Был предложен протокол Royal Holloway, использующий криптографию с открытым ключом, но он вызвал споры из-за сложности управления ключами и потенциальных уязвимостей.

Безопасность платформы

По мере того как мобильные телефоны превращаются в полноценные компьютеры (с ОС Symbian, Windows Mobile), они сталкиваются с теми же проблемами, что и ПК: вредоносное ПО, ботнеты и эксплойты.
Операторы и производители пытаются внедрять DRM (управление цифровыми правами) и контролировать аксессуары (например, блокируя сторонние аккумуляторы). Возникает конфликт: производители блокируют телефоны под конкретного оператора (lock-in), чтобы получать прибыль, а пользователи и хакеры создают инструменты для разблокировки (unlocking), что приводит к юридическим баталиям.

Была ли мобильная безопасность успехом или провалом?

Ответ зависит от того, кого вы спрашиваете:

- **Криптографы** считают ее провалом, так как базовые алгоритмы (Comp128, A5) были взломаны.
- **Телефонные компании** считают ее успехом, так как клонирование остановлено, а доходы растут.
- **Полиция** считает ее провалом, потому что распространение предоплаченных (анонимных) SIM-карт сделало прослушку и отслеживание преступников крайне сложным.

(Voice over IP)

Голосовая связь через IP (VOIP) стала новой реальностью. Однако здесь технические проблемы (задержки, джиттер) переплетаются с экономическими. Традиционные телефонные компании, которые также являются провайдерами интернета, часто пытаются блокировать или ухудшать качество VOIP-трафика, чтобы защитить свои доходы от междугородних звонков. Это порождает споры о «сетевом нейтралитете» (net neutrality).

Экономика безопасности телекоммуникаций

Телекоммуникационный бизнес характеризуется высокими фиксированными затратами и почти нулевыми предельными издержками. Это ведет к ценовой дискриминации и «запутывающему ценообразованию» (confusion pricing), когда операторы усложняют тарифы, чтобы максимизировать прибыль, что, в свою очередь, создает почву для мошенничества.

Мошенничество со стороны телефонных компаний

Потребители часто думают, что мошенничают только хакеры, но сами телефонные компании также занимаются недобросовестными практиками:

- **Cramming (Навязывание):** Операторы добавляют в счет мелкие суммы за якобы оказанные премиальные услуги (гороскопы, игры), которые абонент не заказывал.
- **Slamming (Подмена):** Незаконное изменение оператора междугородней связи абонента без его ведома.
- **Fly-by-night (Компании-однодневки):** Создание подставных компаний для сбора платежей за премиум-услуги, после чего компания исчезает, не перечисляя деньги провайдерам связи.
- **Short termination (Короткое завершение):** Мошенническая схема, при которой звонки маршрутизируются через фиктивные международные номера (например, в Молдове или на Карибах), чтобы избежать оплаты внутренних междугородних тарифов. Знаменитая «Молдавская афера» с порно-сайтами использовала именно эту уязвимость биллинга.

Механизмы биллинга

Защита биллинговых систем критична. Запись о звонке (Call Detail Record, CDR) обычно генерируется только после того, как вызов завершен. Это создает уязвимость для атак с использованием длинных конференц-связей: мошенник создает бесконечную конференцию, и счет за нее не выставляется, пока звонок не будет сброшен.
Для защиты требуются механизмы «тиковых платежей» (tick payments) или онлайн-контроль затрат, но внедрение их в унаследованные телефонные сети (SS7) крайне сложно и дорого.

Итоги

История безопасности телекоммуникаций показывает, что переход от аналоговых к цифровым системам не решил проблем, а лишь изменил их природу. Если раньше основными угрозами были перехват аналогового сигнала и кража услуг, то теперь на первый план вышли проблемы криптографических реализаций (в GSM), конфиденциальности метаданных (IMSI-catchers) и экономическое мошенничество в биллинговых системах.
Главный урок заключается в том, что безопасность телекоммуникаций больше не является исключительно технической задачей. Это комплексная проблема, включающая бизнес-модели операторов, законодательное регулирование

(например, требования по прослушке) и психологию пользователей. Инженер по безопасности должен понимать, что идеальная криптографическая защита может быть полностью нивелирована жадностью операторов, создающих дыры в биллинге, или политическими требованиями, заставляющими внедрять уязвимые бэкдоры.