УДК 004.056

# Аутентификация в сетях сотовой связи: эволюция, обзор способов защиты и новые уязвимости

Бойко А. А., Быков М. Ю., Кущев С. С., Перегудов М. А.

***Постановка задачи:*** *большинство компьютерных атак на сети сотовой связи стандартов AMPS, NMT, GSM, UMTS, LTE, 5G начинается с эксплуатации уязвимостей их процедур аутентификации, которые позволяют перехватывать, просматривать и модифицировать информацию пользователей. Вопросам безопасности сетей сотовой связи посвящено множество работ. Несмотря на достаточно глубокую практическую проработку, они имеют фрагментный характер, не позволяющий проследить эволюцию процедур аутентификации в сетях сотовой связи от первого до текущего поколений и средств эксплуатации уязвимостей этих процедур.* ***Целью работы*** *является анализ процедур аутентификации сетей сотовой связи на предмет систематизации их известных уязвимостей, выявления новых уязвимостей и закономерности в характере происхождения уязвимостей в интересах прогнозирования дальнейшего развития соответствующих средств реализации компьютерных атак и разработки эффективных способов противодействия им.* ***Используемые методы:*** *метод системного анализа, метод генерации кибератак на телекоммуникационное оборудование.* ***Новизна:*** *выявлены новые, ранее не исследованные потенциальные уязвимости процедур аутентификации сетей сотовой связи различных поколений.* ***Результат:*** *обоснована необходимость совершенствования процедур аутентификации в сетях сотовой связи с учетом выявленных уязвимостей.* ***Практическая значимость:*** *результат работы является побудительным фактором для повышения эффективности противодействия средствам реализации уязвимостей процедур аутентификации в сетях сотовой связи.*

***Ключевые слова:*** *система сотовой связи, процедура аутентификации, уязвимость, IMSI-перехватчик, AMPS, NMT, GSM, UMTS, LTE, 5G.*

## Актуальность

С момента создания сотовая связь, ставшая неотъемлемой частью нашей повседневной жизни, претерпела значительную эволюцию своих возможностей. Сегодня в мире основными стандартами сотовой связи остаются стандарты поколений 2G, 3G и 4G [1, 2, 3], и активно внедряется стандарт 5G [4] (сети 6G пока только концепция). Согласно данным фирмы Cisco в 2023 году количество абонентов сотовой связи во всем мире составило около 5,7 млрд [5].

Предоставление услуг сотовой связи изначально подразумевает высокий уровень качества связи и защиты данных пользователей. Однако в стандартах сотовой связи присутствуют уязвимости, использование которых в интересах диверсионной, террористической или иной противоправной деятельности может повлечь серьезные последствия. Так, например, американские военные в Йемене, Сомали и Афганистане используют технологии отслеживания мета-

**Библиографическая ссылка на статью:**
Бойко А. А., Быков М. Ю., Кущев С. С., Перегудов М. А. Аутентификация в сетях сотовой связи: эволюция, обзор способов защиты и новые уязвимости // Системы управления, связи и безопасности. 2024. № 4. С. 95-144. DOI: 10.24412/2410-9916-2024-4-95-144

**Reference for citation:**
Boyko A. A., Bykov M. Yu., Kuschev S. S., Peregudov M. A. Authentication in Cellular Networks: Evolution, Review of Security Methods and New Vulnerabilities. *Systems of Control, Communication and Security*, 2024, no. 4, pp. 95-144 (in Russian). DOI: 10.24412/2410-9916-2024-4-95-144

данных идентификационных модулей пользователей (Subscriber Identity Module, SIM), т.е. SIM-карт, для локализации целей перед их уничтожением беспилотными летательными аппаратами [6], а в 2019 году сотрудниками Министерства внутренней безопасности США возле Белого дома обнаружены устройства перехвата информации с мобильных устройств Д. Трампа [7].

Подавляющее большинство атак на сети сотовой связи начинается с эксплуатации уязвимостей их процедур аутентификации (т.е. проверки подлинности пользователя) [8, 9, 10]. По этой причине исследование вопроса уязвимости этих процедур является актуальным.

## Постановка задачи

На сегодняшний день существует ряд публикаций, в которых содержится обзор уязвимостей сетей сотовой связи.

Обзор механизмов защиты и уязвимостей в сети сотовой связи стандарта второго поколения GSM (Global System for Mobile Communications) рассмотрен в работах **И. А. Хамцова** [8] и **В. С. Яковлева** [13]. В своих исследованиях авторы описывают механизмы обеспечения безопасности и частично уязвимости в сетях сотовой связи второго поколения. Однако в данных работах отсутствует системный подход, предусматривающий рассмотрение всех существенных внутренних процессов элементов сети в процедуре аутентификации. Это не позволяет изучить уязвимые места таких элементов и тем самым разработать комплексные меры по защите от угроз.

В статье [9] **M. Khan**, **A. Ahmed** и **A. Cheema** рассматривают уязвимости в архитектуре безопасности стандарта UMTS (Universal Mobile Telecommunications System), позволяющие реализовать в сети атаки типа «человек посередине» (man-in-the-middle), атаки типа «отказ в обслуживании» (Denial-of-Service, DoS), т.е. DoS-атаки, и перехват значения международного идентификационного номера абонента (International Mobile Subscriber Identity, IMSI). Но в ней рассматриваются только уязвимости аутентификации в протоколе управления радиоресурсами (Radio Resource Control, RRC), хотя в стандарте UMTS существуют и многие другие уязвимости аутентификации.

В статье [11] **K. Kareem** анализирует уязвимости в процедуре аутентификации в сетях сотовой связи 4G и 5G, которые используются т.н. «IMSI-перехватчиками», входящими в состав используемых злоумышленниками т.н. «виртуальных базовых станций». Однако в [11] не рассмотрены уязвимости в процедуре аутентификации, связанные с сообщениями о сбоях протокола совместной выработки ключа (Authentication and Key Agreement, AKA), а также уязвимости, возникающие в результате повторного переназначения глобального уникального временного идентификатора (Globally Unique Temporary Identifier, GUTI). Кроме того, в [11] не исследуется возможность перехвата постоянного (Subscription Permanent Identifier, SUPI) и скрытого (Subscription Concealed Identifier, SUCI) идентификаторов абонента.

В работе [12] **F. V. Broek**, **R. Verdult** и **J. D. Ruiter** рассмотрели угрозы применения IMSI-перехватчиков в сетях сотовой связи второго, третьего и четвертого поколений. Тем не менее, в этой работе авторы не отслеживают эволю-

цию систем безопасности в различных поколениях сотовой связи и предлагают лишь один подход к решению проблемы, не рассматривая альтернативные методы защиты или комплексные подходы к повышению уровня безопасности. Кроме того, как и в [11], в работе [12] не рассматриваются уязвимости, связанные с сообщениями о сбоях протокола AKA, а также атаки повторного переназначения идентификатора *GUTI* и риски, связанные с перехватом идентификаторов *SUPI* или *SUCI*. Здесь и далее курсивом выделяются те аббревиатуры, которые обозначают численное значение соответствующего показателя.

В работе [14] **Д. О. Мазуркевич** рассмотрел процедуры аутентификации в сетях сотовой связи первого, второго и третьего поколений. Однако в ней отсутствует детальное описание всех этапов этих процедур, что не позволяет проанализировать возможные угрозы для процедур аутентификации и достаточность известных соответствующих им мер защиты.

В статье о безопасности стандарта LTE (Long-Term Evolution) [15] **М. И. Данилин** рассмотрел такие атаки, как интерференция, подавление сигнала, клонирование SIM-карт расширенного стандарта (Universal Subscriber Identity Module, USIM), атака определения местоположения пользователя и атака на полосу пропускания. Однако в этой работе не содержится описание принципов эксплуатации уязвимостей, связанных с процедурами аутентификации, а также возникающих угроз вследствие их эксплуатации.

В статье [16] **В. С. Бельский**, **А. В. Дрынкин** и **С. А. Давыдов** рассматривают вопросы обеспечения безопасности абонентов в системах сотовой связи 5G, анализируют уязвимости и угрозы, унаследованные от предыдущих поколений и возникшие в новом стандарте. Эта работа весьма глубоко проработана с практической точки зрения и отличается логически выстроенной структурой. Однако в ней не учтены аспекты DoS-атак и использование т.н. «виртуальных базовых станций».

В целом имеющиеся работы, несмотря на достаточно глубокую проработку, тем не менее имеют фрагментный характер, не позволяющий проследить эволюцию процедур аутентификации в сетях сотовой связи от первого до текущего поколений и средств эксплуатации уязвимостей этих процедур.

Цель работы – анализ процедур аутентификации сетей сотовой связи на предмет систематизации их известных уязвимостей, выявления новых уязвимостей и закономерности в характере происхождения уязвимостей в интересах прогнозирования дальнейшего развития соответствующих средств реализации компьютерных атак и разработки эффективных способов противодействия им.

## 1. Анализ уязвимостей аутентификации сетей сотовой связи 1G

Сотовая связь первого поколения представлена стандартами AMPS (Advanced Mobile Phone System) и NMT (Nordic Mobile Telephony). Они обеспечивают предоставление всего одной услуги – телефонии. Архитектура сетей AMPS и NMT имела довольно простой вид, показанный на рис. 1.

В связи с ускоренным темпом внедрения AMPS и NMT в 1990-х годах проявились серьезные уязвимости безопасности сетей сотовой связи, формируемых на основе этих стандартов. Предпосылки состояли в следующем.


Рис. 1. Архитектура сетей сотовой связи первого поколения

В сетях AMPS отсутствовало шифрование данных, и безопасность информации обеспечивалась путем использования двух параметров:

1) электронный серийный номер (Electronic Serial Number, ESN) [17];
2) мобильный идентификационный номер (Mobile Identification Number, MIN) [18].

*ESN* присваивался производителем устройства, а *MIN* присваивался оператором сети. Процесс аутентификации в сетях первого поколения основан на приеме базовой станцией идентификаторов *ESN* и *MIN* от мобильного терминала на определенной частоте.

В NMT использовалось скремблирование голоса на мобильном телефоне и базовой станции [19]. Это не было достаточным способом защиты информации, но предотвращало атаки низкоквалифицированных злоумышленников, перехватывающих звонки.

Исходя из этого, основными уязвимостями аутентификации в сетях сотовой связи первого поколения являлись:

1) отсутствие параметров, подтверждающих легитимность использования ресурсов сети пользователем;
2) передача данных в незашифрованном виде.

Такие уязвимости порождали следующие угрозы безопасности:

1) подделка идентификаторов: в сетях стандарта AMPS злоумышленник мог (сейчас такие сети не используются) перехватить в эфире звонки, извлечь идентификаторы *MIN* и *ESN* и подделать терминал абонента для того, чтобы выдать себя за другого абонента. Из-за этого операторы сетей сотовой связи стандарта AMPS несли значительные убытки;
2) перехват и модификация сообщений: злоумышленник мог перехватить передаваемые данные между клиентом и базовой станцией и модифицировать их содержимое;
3) отказ в обслуживании (т.е. DoS-атака): атакующий мог создать большой объем запросов, что приводило к невозможности обслуживания легитимных клиентов.

Последствия реализации таких угроз:

1) потеря конфиденциальности клиентской информации;
2) нарушение целостности передаваемых в системе связи сообщений;
3) периодическое нарушение доступности системы связи;
4) потеря доверия клиентов.

Ввиду того, что сети сотовой связи первого поколения в настоящее время не используются, новые уязвимости в них анализировать не целесообразно.

## 2. Анализ уязвимостей аутентификации сетей сотовой связи 2G

Разработка стандартов сотовой связи второго поколения стартовала в начале 1980-х годов. Примером является стандарт GSM. Под сетями GSM так же понимаются и сети DCS (Digital Cellular System), работающие аналогично на более высоком диапазоне частот.

Услуги сетей стандарта GSM: голосовые звонки, передача коротких текстовых сообщений, мультимедийные сообщения, голосовая почта, определение вызывающего номера и ограничение такого определения, переадресация вызова на другой номер, ожидание и удержание вызова. В отличие от сетей первого поколения в GSM появился центр аутентификации и закрытые ключи, которые хранятся на мобильной станции и базовой станции. В GSM используются следующие механизмы обеспечения безопасности:

1) аутентификация: защищает оператора сети и мобильного абонента от несанкционированного использования ресурсов сети и абонента;
2) шифрование данных: для предотвращения перехвата радиопереговоров используются три алгоритма шифрования: A3 (аутентификация), A5 (непосредственное шифрование разговоров) и A8 (генерация сеансового ключа);
3) выдача временного идентификатора мобильного абонента (Temporary Mobile Subscriber Identity, TMSI): защищает абонента от несанкционированной идентификации;
4) проверка интернационального идентификатора мобильной станции (International Mobile Equipment Identity, IMEI): предотвращает использование украденной/несанкционированной мобильной станции.

В процедуре аутентификации GSM используются 5 элементов сети [20]:

1) мобильная станция (Mobile Station, MS);
2) базовая станция (Base Transceiver Station, BTS) – это оборудование, которое обеспечивает радиосвязь MS и сети;
3) визитный регистр местоположения (Visitor Location Register, VLR) – это элемент сети, который хранит информацию о местоположении всех активных MS сети;
4) домашний регистр местоположения (Home Location Register, HLR) – это элемент сети, который хранит постоянную информацию об абонентах мобильной сети, такую как их идентификационные данные, подключенные и запрещенные услуги, местоположение;
5) центр аутентификации (Authentication Center, AuC) – это элемент сети GSM, который отвечает за предоставление информации об абонентах сети и генерацию ключей шифрования для выполнения процедуры аутентификации между MS и сетью.

Главное усовершенствование стандартов 2G перед 1G в том, что параметры аутентификации записаны на SIM-карте, а не на MS [21]. В памяти SIM-карты хранятся следующие параметры аутентификации [22]:

1) международный идентификационный номер абонента (International Mobile Subscriber Identity, IMSI);

№4. 2024
ISSN 2410-9916

2) индивидуальный секретный ключ ($K_i$);
3) программа выполнения алгоритма шифрования A3.

В AuC о каждом абоненте изначально содержатся следующие данные: *IMSI* и индивидуальный секретный ключ ($K_i$). AuC в ходе своей работы генерирует следующий т.н. «триплет» (т.е. три параметра) аутентификации:

1) *RAND* – случайное значение в каждом сеансе аутентификации. Для генерации 128-битного значения *RAND* используется секретный ключ $K_i$;
2) *XRES* – ожидаемый SIM-картой ответ от AuC в текущем сеансе аутентификации. Он создается с использованием алгоритма A3 на основании сгенерированного значения *RAND* и секретного ключа $K_i$;
3) $K_C$ – сеансовый ключ, который генерируется для каждого сеанса аутентификации с использованием алгоритма A8.

**Процедура аутентификации в GSM** состоит из следующих девяти этапов, показанных на рис. 2 [23]. Рассмотрим их.

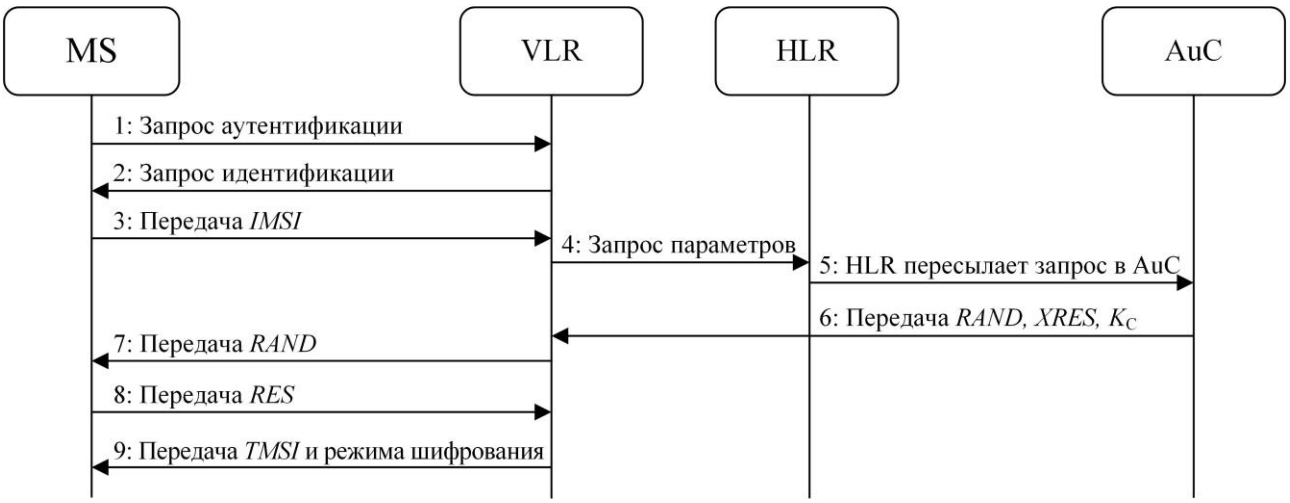


Рис. 2. Процедура аутентификации в сети GSM

Этап 1. MS абонента через BTS делает запрос в VLR на аутентификацию, в котором указывает свои доступные режимы шифрования.

Этап 2. VLR отправляет MS запрос идентификации, запрашивая *IMSI*.

Этап 3. MS отправляет свой *IMSI* на VLR. Структура *IMSI* показана на рис. 3 [24].

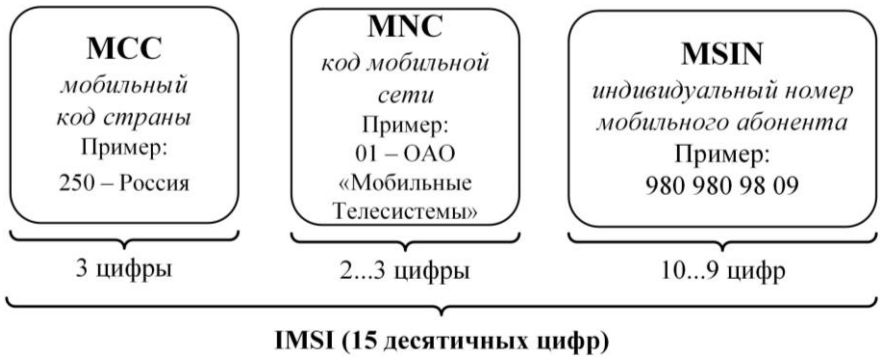


Рис. 3. Структура *IMSI*

Этап 4. VLR делает запрос параметров аутентификации в HLR.

DOI: 10.24411/2410-9916-2024-4-95-144
URL: https://sccs.intelgr.com/archive/2024-04/04-Boyko.pdf

Этап 5. HLR пересылает запрос в AuC.

Этап 6. AuC генерирует 128-битное случайное число *RAND*. После этого в AuC вычисляется ответ *XRES* на основе *RAND* и индивидуального ключа $K_i$, который соответствует SIM-карте MS абонента (см. рис. 4):

$$XRES = A3 (K_i, RAND). \quad (1)$$

Далее триплет *RAND*, *XRES* и $K_C$ из AuC отправляется обратно в VLR.

Этап 7. VLR, получив триплет, отправляет на MS только значение *RAND*.

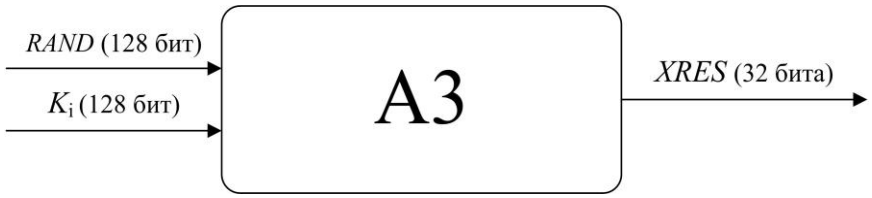


Рис. 4. Вычисление значения *XRES* в центре аутентификации

Этап 8. MS, получив значение *RAND*, вычисляет значение параметра *RES* с помощью алгоритма A3:

$$RES = A3 (K_i, RAND). \quad (2)$$

После этого MS отправляет ответный сигнал *RES* на VLR.

Этап 9. В VLR происходит сравнение значений *RES* и *XRES*. Если значения совпадают, то MS подключается к сети. В противоположном случае запрос на аутентификацию отклоняется. VLR присваивает мобильной станции *TMSI* и устанавливает один из следующих алгоритмов шифрования (режимов):

- A5/0 – режим работы, когда шифрования в принципе нет. Этот режим предназначен для применения в странах, где законы не разрешают применение криптостойких алгоритмов шифрования;
- A5/1 – алгоритм шифрования для Северной Америки и Европы. В его реализации найдены уязвимости, позволяющие его взломать с помощью т.н. «радужных таблиц» [25, 26]. Для реализации такой атаки достаточно ЭВМ с 2 Гбайт оперативной памяти и жестким диском объемом 2 Тбайт. Это позволит получить секретный ключ за 2 мин;
- A5/2 – более слабый алгоритм шифрования в сравнении с A5/1. Разработан для использования в странах, где ограничения могут препятствовать использованию A5/1. С 2006 года в сетях GSM этот алгоритм не используется [27];
- A5/3 (также имеет название KASUMI) – наиболее криптостойкий алгоритм шифрования с открытым ключом. Однако ряд исследований показал возможность вскрытия данного алгоритма методами невозможных дифференциалов [28], бумеранга [29] и с использованием атаки на основе связанных ключей [30].

После этого VLR отправляет *TMSI* и установленный режим шифрования на MS абонента. Если выбрано любое шифрование, отличное от A5/0, то MS абонента создает сеансовый ключ $K_C$ на основе алгоритма шифрования A8 и ранее сгенерированного значения *RAND*. Сеансовый ключ $K_C$ остается актуальным, пока не поступит новый запрос на аутентификацию.

Одной из основных угроз в сетях GSM являются средства, обеспечивающие перехват в радиоканале (в зоне радиодоступности) значения *IMSI*. Они называются «IMSI-перехватчиками» и часто входят в состав виртуальных базовых станций, дублирующих функции легитимных базовых станций. IMSI-перехватчики используют атаки типа «человек посередине», одновременно выступая в роли MS для легитимной BTS, чтобы получить ее данные, и BTS для MS абонента, чтобы получить ее данные. Наиболее известным образцом IMSI-перехватчика являются устройства серии StingRay, производимые корпорацией L3Harris для правоохранительных, военных и разведывательных органов США. Изначально такие устройства продавались только для государственных структур. Но в 2013 году в результате утечки данных стало известно, что международная компания Gamma Group разработала нательный вариант IMSI-перехватчика. Со временем принцип работы этих устройств стал открытым, что позволило производить их частным лицам и создало серьезную угрозу для широких масс абонентов сетей сотовой связи. Сегодня такие устройства из-за их широкого распространения могут использоваться не только правоохранительными органами, но и злоумышленниками для корпоративного шпионажа, диверсантами и террористами.

Принцип работы IMSI-перехватчиков основан на использовании уязвимости в процедуре выбора базовой станции MS абонента. Если в радиусе доступности мобильного телефона находятся несколько BTS, то MS обычно подключаются к BTS, которая излучает наиболее привлекательный (не только более мощный) сигнал. Кроме того, BTS и зона обслуживания, к которой она принадлежит, не должны находиться в списке запрещенных BTS.

IMSI-перехватчики создают сигналы BTS с такими физическими и информационными параметрами (см., например, [31]), которые позволяют привлечь к себе подключение MS независимо от их оператора сотовой связи [32]. Когда MS обнаруживает такой сигнал, она подключается к IMSI-перехватчику, рассматривая его как наиболее подходящую BTS в радиусе своего действия. После подключения IMSI-перехватчик может получить *IMSI* мобильной станции, отключить шифрование и провести анализ полученных данных.

Процедура работы IMSI-перехватчика в сети GSM представлена на рис. 5 и состоит из следующих четырнадцати этапов, выполняемых в отношении всех энергодоступных MS сотовой связи в заданном районе [32].

Этап 1. MS передает на IMSI-перехватчик список поддерживаемых алгоритмов шифрования A5.

Этап 2. IMSI-перехватчик отправляет MS команду запроса идентификации.

Этап 3. MS отправляет свой *IMSI*.

Этап 4. IMSI-перехватчик высылает значение *RAND* мобильной станции.

Этап 5. MS высылает свое значение *RES*.

Этап 6. IMSI-перехватчик присылает мобильной станции *TMSI* и включает режим A5/0 (то есть шифрование отключено).

Этап 7. IMSI-перехватчик подключается к сети, отправляя запрос на обновление местоположения.

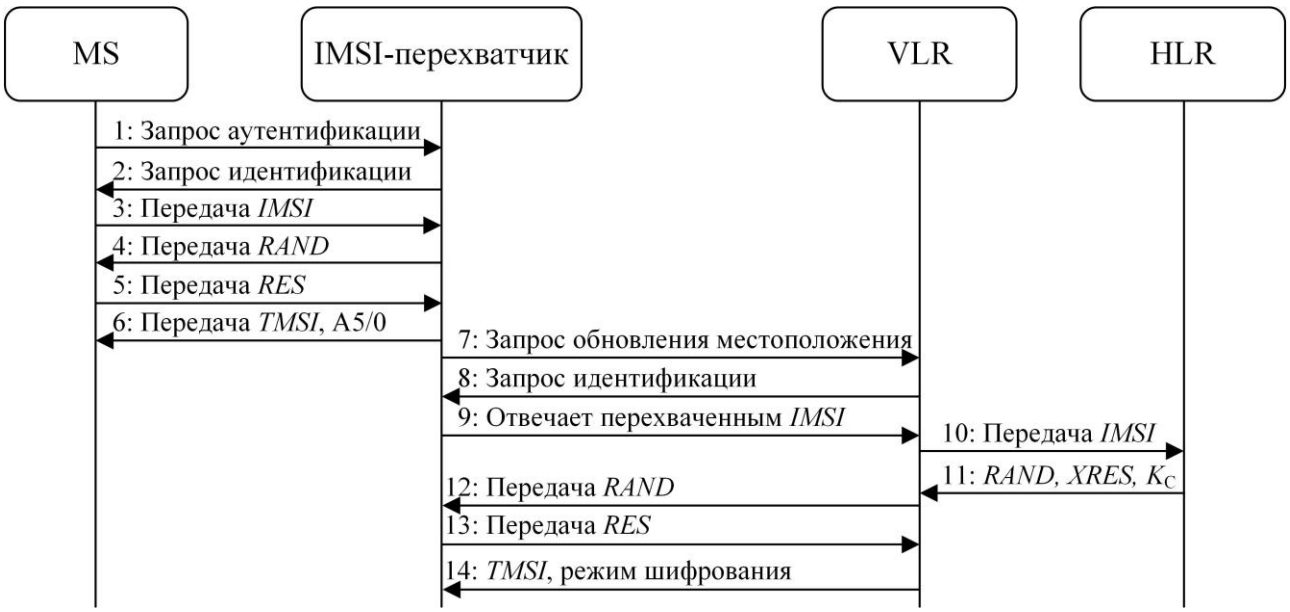


Рис. 5. Процедура работы IMSI-перехватчика в сети стандарта GSM

Этап 8. Сеть делает запрос идентификации, запрашивая *IMSI*.

Этап 9. IMSI-перехватчик отвечает украденным *IMSI* мобильной станции.

Этап 10. VLR отправляет данные аутентификации на HLR.

Этап 11. HLR присылает в ответ *RAND*, *XRES* и ключ $K_C$.

Этап 12. VLR отправляет *RAND* на IMSI-перехватчик.

Этап 13. IMSI-перехватчик отправляет *RES* на VLR. Если *RES* и *XRES* не совпадают, то запрос аутентификации отклоняется. В противном случае он принимается.

Этап 14. VLR присваивает IMSI-перехватчику временный идентификатор мобильного абонента *TMSI* и сообщает ему, какой из алгоритмов шифрования A5 использовать.

После завершения процедуры подключения IMSI-перехватчика к MS абонента он исключает возможность подключения этой станции к другим BTS сети. Легитимные BTS предоставляют информацию о соседних BTS, которые находятся вблизи абонента. Это необходимо для плавного переключения абонента между ячейками сети. Поведение IMSI-перехватчика в большинстве случаев отличается от поведения легитимной BTS тем, что MS абонента получает пустой список соседних ячеек.

В процессе анализа процедуры аутентификации сетей GSM стали общеизвестными следующие уязвимости.

1. Низкая криптостойкость алгоритмов шифрования данных. Алгоритмы шифрования исследовались криптоаналитиками длительное время [33]. После утечки информации, которая содержала архитектуру и принцип работы алгоритма A5/1, специалисты в области информационной безопасности опубликовали результаты исследования, раскрывающие уязвимости в работе этого алгоритма и возможные сценарии соответствующих атак. В 1997 году своей работе [34] **J. D. Golic** предложил атаку, основанную на компромиссе времени и памяти (Time/memory/data tradeoff attack, TMTO). Для успешного выполнения предложенной атаки необходимо либо 15 ТБайт заранее подготовленных данных,

либо 3 часа известных разговоров, что является маловероятным в реальных условиях. В 2001 году **A. Biryukov, A. Shamir** и **D. Wagner** в работе [35] представили атаку, также использующую компромисс времени и памяти, требуя 2 с открытых данных и несколько минут для обработки. В 2003 году этот тип атаки усовершенствовали **E. Barkan**, **E. Biham** и **N. Keller** в работе [36]. Для реализации их атаки необходимо было иметь несколько десятков миллисекунд зашифрованного разговора. С помощью предложенного метода правильный ключ на персональном компьютере находился менее чем за 1 с. В том же 2003 году в работе [37] **P. Ekdahl** и **T. Johansson** предложили другую стратегию, основанную на корреляционной атаке. Основное преимущество этой атаки в том, что, в отличие от атак на основе компромисса времени и памяти (TMTO), её сложность ничтожно мало зависит от длины сдвигового регистра. В 2004 году эту атаку дополнительно улучшили **A. Maximov** и **T. Johansson** в работе [38]. В результате атака требовала менее 1 мин вычислений. Тем не менее все перечисленные атаки имели высокие требования к вычислительной технике и основывались на сложно реализуемых допущениях. В работе [39] **K. Nohl** и **S. Munaut** парировали эти недостатки, впервые предложив использовать радужные таблицы для извлечения ключа из канала связи в реальном времени.

2. В работе [40] **V. Bocan** и **V. Cretu** показали, что злоумышленник может использовать перехваченные или сгенерированные *IMSI* для осуществления DoS-атаки и DDoS-атаки (Distributed Denial of Service, т.е. распределенный отказ в обслуживании), запрашивая регистрацию абонентов в сети, что может вызвать перегрузку сети. Этот тип атаки проводится как с использованием случайных значений *IMSI*, так и целенаправленно на *IMSI* конкретного оператора.

3. В работе [41] **М. А. Перегудов**, **А. Я. Уманский**, **А. А. Жданова** и **В. Ю. Храмов** показали, что IMSI-перехватчик виртуальной базовой станции может перехватить ключ и информацию о режиме шифрования. В результате может быть назначен неверный ключ шифрования для абонента, что вызовет сбои в работе сети. Получив режим шифрования, IMSI-перехватчик может извлечь информацию о MS и принудительно перевести ее на использование алгоритма A5/0 (т.е. отключить шифрование). Эта уязвимость позволяет злоумышленнику перехватывать и анализировать информацию в сети.

4. В работе [42] **S. Wray** показал, что, отправляя значения *RAND* на MS, IMSI-перехватчик может вычислить $K_i$, получая значения *RES* и отправляя их на BTS для проверки аутентификации (см. рис. 6). Алгоритм A8 и его реализация COMP128 имеет уязвимости, позволяющие злоумышленникам извлекать секретный ключ $K_i$. Исследования показали, что с помощью примерно 150 000 запросов и анализа полученных значений возможно восстановить секретный ключ $K_i$. В зависимости от условий время выполнения такого количества запросов может варьироваться от 4 ч до более чем 20 ч. Применение оптимизированного оборудования и методов может значительно ускорить атаку, особенно если создать клон SIM-карты. Это сократит время перебора и ускорит процесс поиска ключа. Компанией Osmocom разработан скрипт osmo-sim-auth, который может быть использован для анализа процесса аутентификации в сетях GSM и UMTS, что теоретически открывает возможности для атак на индивидуальный

ключ SIM-карты ($K_i$). Хотя сам скрипт не предоставляет прямого доступа к этому секретному ключу, злоумышленник может использовать его для отправки множественных запросов аутентификации с различными значениями случайного числа *RAND* и анализировать полученные ответы *RES*. Путем систематического перебора и анализа полученных данных возможно восстановление информации, необходимой для компрометации ключа. Если *RES* совпадает с тем, что рассчитывает BTS на основе правильного значения $K_i$, то аутентификация проходит успешно. Если совпадения нет, то злоумышленник получает информацию о том, что использованное значение *IMSI* не зарегистрировано, или если он получает ошибку аутентификации, то переходит к следующему значению, повторяя операции.


Рис. 6. Алгоритм вычисления индивидуального ключа $K_i$

5. Отсутствие взаимной аутентификации. В работе [41] **М. А. Перегудов**, **А. Я. Уманский**, **А. А. Жданова** и **В. Ю. Храмов** также показали, что MS аутентифицирует себя, не проверяя легитимность используемой BTS. Это позволяет злоумышленнику подключать своё устройство, осуществляя атаку «человек посередине».

Для выявления новых потенциально возможных уязвимостей процедур аутентификации сетей сотовой связи в настоящем исследовании использован метод генерации кибератак (т.е. компьютерных атак) на телекоммуникационное оборудование, предложенный **А. А. Бойко** в работе [43]. Идея этого метода состоит в том, что необходимое и достаточное множество тестовых способов реализации кибератак на телекоммуникационное оборудование при известном протоколе (т.е. алгоритмах передачи информации) формируется путем комбинаторного сочетания параметров своевременности доставки, кратности передачи и точности содержания сообщений, регламентируемых этим протоколом. Под телекоммуникационным оборудованием здесь понимается множество взаимодействующих по заданному протоколу информационно-технических средств, т.е. радиоэлектронных средств, средств вычислительной техники или их конструктивно единая комбинация друг с другом или со средствами электронной автоматики. Содержание этого метода показано на рис. 7.

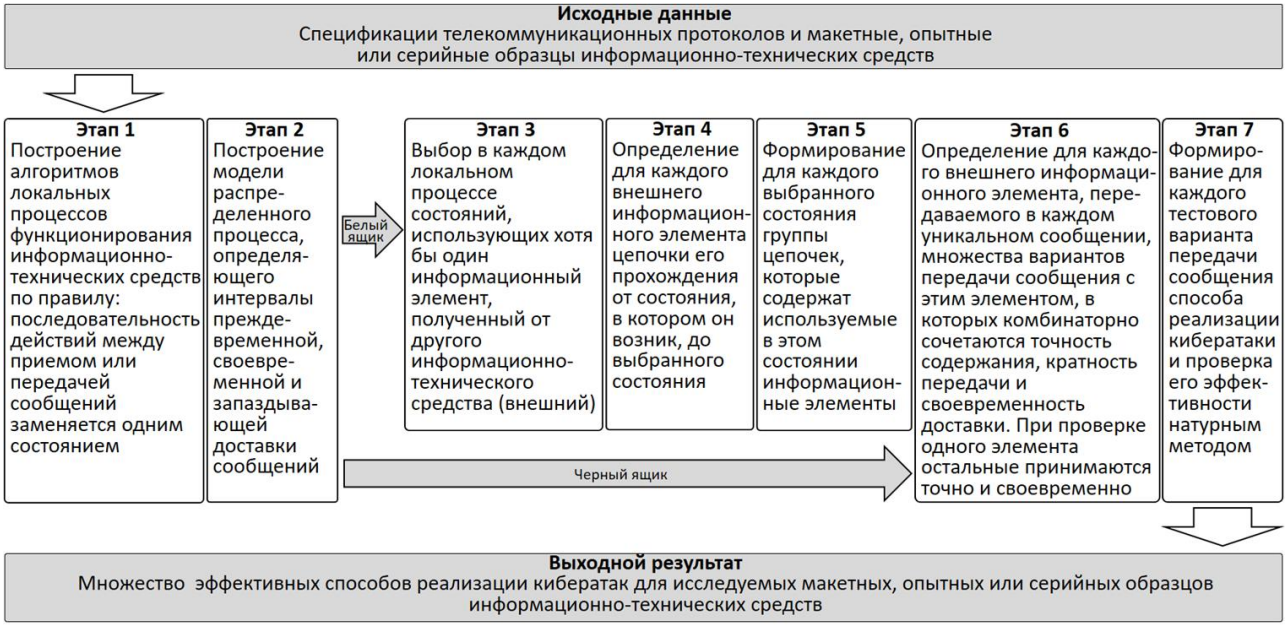


Рис. 7. Содержание метода генерации кибератак на телекоммуникационное оборудование

В контексте настоящего исследования первоочередной интерес представляет шестой этап метода, предусматривающий определение для каждого внешнего информационного элемента (например, *RAND*), передаваемого в каждом уникальном сообщении, множества вариантов передачи этого сообщения, в которых комбинаторно сочетаются точность содержания, кратность передачи и своевременность доставки согласно пространству вариантов на рис. 8.

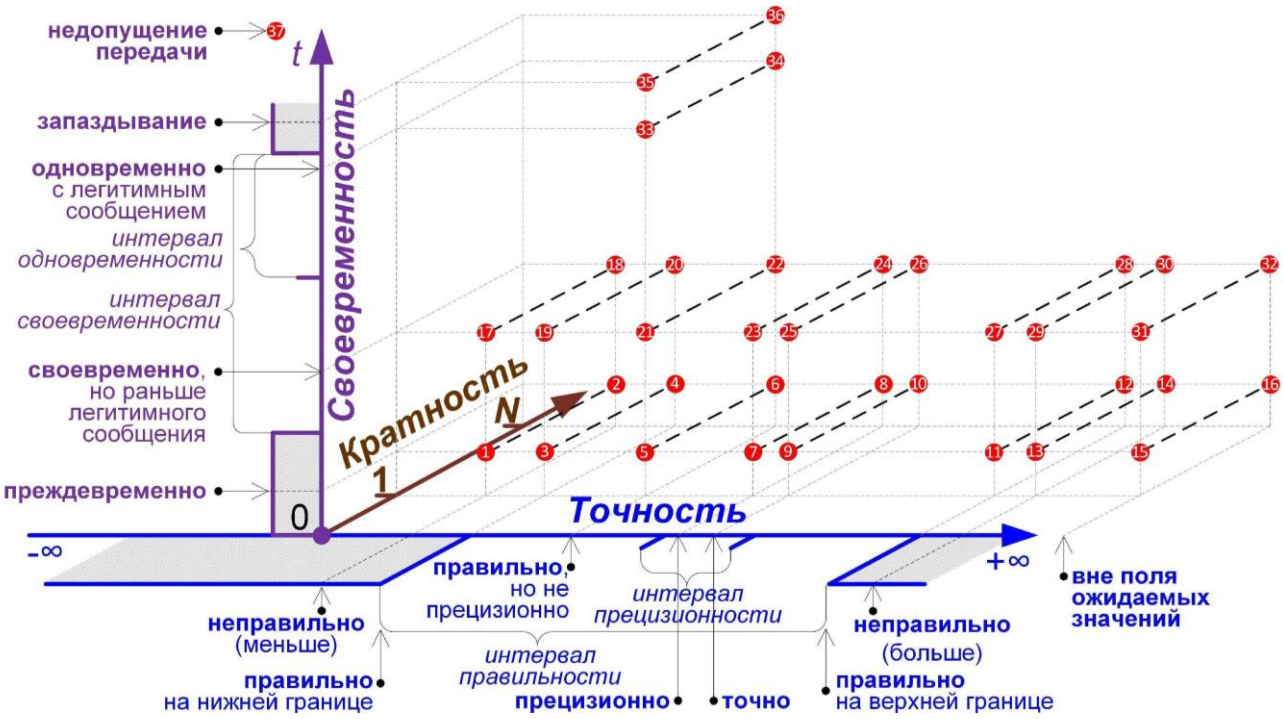


Рис. 8. Пространство вариантов передачи сообщения в тестовых способах реализации компьютерных атак

С использованием метода генерации кибератак на телекоммуникационное оборудование выявлены следующие ранее не исследованные уязвимости безопасности процедуры аутентификации сетей сотовой связи стандарта GSM.

1. Перехват запроса аутентификации от MS к сети. Злоумышленник способен влиять:

а) на точность содержания сообщений: используя содержимое перехваченных параметров, злоумышленник имеет возможность их прочитать или изменить. Мониторинг подключаемых абонентов позволяет создать базу абонентов сети для дальнейших атак: отслеживание нахождения этих абонентов в зоне действия, пролистывание IMSI (IMSI-paging) и зондирование IMSI (IMSI-probing), мониторинг активности по количеству запросов аутентификации. Кроме того, при передаче *IMSI* возможно определить код страны и оператора подключаемого абонента. Если MS передает *TMSI* вместе с идентификатором локальной зоны (Local Area Identificator, LAI), то злоумышленник также может записать информацию абонента для осуществления перечисленных выше атак. В случае перемещения абонента в другую зону злоумышленник может осуществить аутентификацию в текущей зоне, зная $K_i$ и имитируя запрос подключения абонента в текущей зоне. Тем самым будет вызван сбой в работе сети. Перехват и модификация передаваемых значений может вызвать отказ в аутентификации, ошибки в обработке информации или переполнение буфера в элементах сети;

б) на кратность передачи: злоумышленник может многократно оправлять собранные ранее или сгенерированные самостоятельно запросы аутентификации, что позволяет ему осуществлять DoS-атаки.

2. Перехват запроса идентификации от сети к MS. Злоумышленник способен влиять:

а) на точность содержания сообщений: модификация сообщения может привести к ошибке аутентификации или переполнению буфера при работе с SIM-картой абонента. Обращаясь к MS абонента по *TMSI*, злоумышленник имеет возможность запросить значения *IMSI*, что позволит деанонимизировать абонента;

б) на кратность передачи: возможно осуществить многократные запросы *IMSI* одного или нескольких абонентов, что будет являться DoS-атакой на соответствующие MS или вызовет ответную реакцию в виде многократных ответов от одного или нескольких абонентов к сети, что по сути также будет являться DoS- или DDoS-атакой.

3. Перехват передачи значения *IMSI* от MS к сети. Злоумышленник способен влиять:

а) на точность содержания сообщений: при переборе сгенерированных значений *IMSI* можно выявить их наличие в базе данных AuC, основываясь на получаемых ответах (см. рис. 9). Если в ответе присутствует значение *RAND*, то этот *IMSI* зарегистрирован в базе. Если происходит ошибка аутентификации, то это указывает на отсутствие такого значения в базе данных. Кроме того, возможно реализовать атаку перебором

значений *RES* для вычисления индивидуального ключа $K_i$ без участия MS абонента, о чем написано в работе [42]. Для атаки злоумышленнику достаточно отправлять запросы аутентификации со значением *IMSI* жертвы, которое было перехвачено ранее или сгенерировано самим злоумышленником. Получая запрос на вычисление ответа *RES* со случайно сгенерированным значением *RAND*, злоумышленник, используя алгоритм A8, вычисляет ответ *RES* и отправляет его для сравнения в сеть, выдавая себя за легитимного пользователя (см. рис. 10). Получив ответ *RES*, сеть сравнивает собственное значение *RES* с полученным. Если ответы совпадают, то аутентификация считается успешной. Если получена ошибка аутентификации, то текущее значение $K_i$ неправильное. Перебирая значения, злоумышленник достигнет значения, позволяющего вычислить правильный ответ *RES* и успешно произвести аутентификацию, что будет означать правильно обнаруженный ключ $K_i$;

б) на кратность передачи: аналогично п. 2 при многократных запросах существует возможность осуществления DoS- и DDoS-атак.

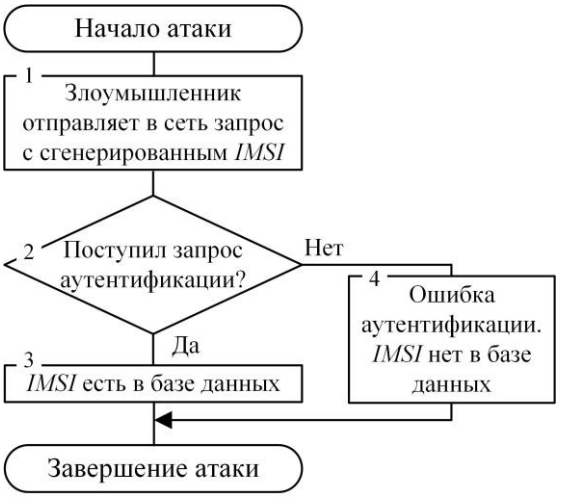


Рис. 9. Алгоритм проверки наличия *IMSI* в базе данных

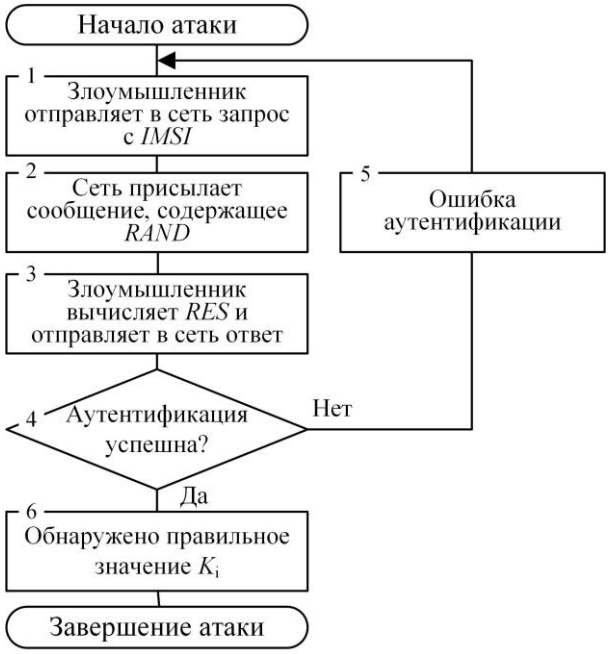


Рис. 10. Алгоритм вычисления ключа $K_i$ методом перебора

4. Перехват передачи значения *RAND* от сети к MS. Злоумышленник способен влиять:

а) на точность содержания сообщений: такое значение передается в открытом виде и без контроля целостности, что позволяет его модифицировать и использовать в атаке перебором для вскрытия индивидуального ключа $K_i$, либо изменять содержимое. Это может вызвать ошибки аутентификации или переполнение буфера на MS абонента;

б) на кратность передачи: многократное выполнение процедуры вычисления значения *RES* может создать нагрузку на вычислительные ресурсы MS.

5. Перехват значения *RES* от MS к сети: Злоумышленник способен влиять:

а) на точность содержания сообщений: такие значения передаются без контроля целостности, что позволяет проводить ряд атак, описанных выше. Также модификация этого значения может вызывать ошибки аутентификации или переполнение буфера в элементах сети;

б) на своевременность доставки: если злоумышленник пришлет раньше MS абонента неправильное значение *RES* на BTS, то это может привести к ошибке аутентификации и завершению процедуры.

Обладая вычисленным значением индивидуального ключа $K_i$, злоумышленник может определить ключ шифрования по формуле:

$$K_C = A8\ (K_i, RAND). \quad (3)$$

Вычислив правильное значение ключа шифрования, злоумышленник имеет возможность перехватывать, дешифровать, изменять и шифровать информацию, не отключая при этом шифрование между MS абонента и сетью. Эта уязвимость существенно снижает вероятность обнаружения атаки за счет исключения критерия обнаружения по индикации отключения шифрования передаваемой информации в сети.

6. Злоумышленник на каждом этапе с использованием средств радиоподавления в соответствующие интервалы времени может задерживать передачу информации как от MS абонентов, так и от обслуживающей сети, что приведет к истечению времени таймера процедуры аутентификации и вызовет ее завершение.

Исходя из рассмотренных выше уязвимостей, злоумышленник получает возможность получения служебной информации обслуживающей сети, включая их временные и постоянные идентификаторы, значения *RAND* и *RES*. На основе этой информации он способен определять код странны и оператора абонента по *IMSI*, активность по количеству запросов, расшифровывать сеансы связи пользователей, используя слабые места в алгоритмах шифрования и используя методы перебора ключей. Используя повторные запросы, злоумышленник может проводить повторные регистрации абонентов в сети, проводить проверки наличия пользователя в сети, выполнять переполнение буфера на оборудовании абонента и обслуживающей сети. Также возможно проводить DoS- и DDoS-атаки на конкретных абонентов сети и элементы обслуживающей сети по случайным значениям или в указанном диапазоне. Безопасность сетей стандарта GSM не обладает достаточной гибкостью, позволяющей модернизировать систему защиты в части устранения выявленных уязвимостей на стороне как абонента, так и оборудования обслуживающей сети.

С учетом вышеизложенного в таблице 1 перечислены уязвимости процедуры аутентификации стандарта GSM, опубликованные ранее и впервые выявленные в ходе настоящего исследования с использованием метода генерации кибератак на телекоммуникационное оборудование.

Таблица 1 – Уязвимости процедуры аутентификации сетей GSM

| № | Уязвимость | Публикации |
|---|---|---|
| 1 | Слабые алгоритмы шифрования | [33, 34, 35, 36, 37, 38, 39] |
| 2 | Отсутствие аутентификации BTS | [42] |
| 3 | Перехват и модификация ключа и режима шифрования | [41] |
| 4 | Изменение содержимого запроса аутентификации от MS к BTS | |
| 5 | Блокирование запроса аутентификации от MS к BTS | |
| 6 | Блокирование запроса идентификации от BTS к MS | |
| 7 | Возможность осуществления DoS- и DDoS-атак, используя запрос к сети и запрос к MS во время инициализации | [40] |
| 8 | Изменение запроса идентификации между от BTS к MS | |
| 9 | Изменение запроса идентификации между от MS к BTS | |
| 10 | Мониторинг подключающихся абонентов к сети | Рассматриваются впервые |
| 11 | Мониторинг интенсивности активности абонентов на основе запросов аутентификации | |
| 12 | Определение кода страны и оператора по *IMSI* | |
| 13 | Повторная аутентификация в зоне, где отсутствует абонент, используя вычисленный ключ $K_i$ | |
| 14 | Завершение процедуры аутентификации, используя модификацию запросов неправильными значениями | |
| 15 | Переполнение буфера в оборудовании сети во время процедуры аутентификации | |
| 16 | Переполнение буфера в MS во время процедуры аутентификации | |
| 17 | Осуществление DoS- и DDoS-атаки легитимными MS абонентов, используя запрос идентификации от BTS | |
| 18 | Проверка наличия *IMSI* в базе на основе полученных ответов от сети | |
| 19 | Вычисление ключа $K_i$ методом перебора на стороне сети | |
| 20 | Отсутствие шифрования значения *RAND* | |
| 21 | Отсутствие контроля целостности значения *RAND* | |
| 22 | Возможность модификации значения *RAND* | |
| 23 | Отсутствие контроля целостности значения *RES* | |
| 24 | Возможность закончить процедуру аутентификации, прислав раньше легитимного пользователя неправильное значение *RES* | |
| 25 | Вычисление ключа шифрования $K_C$, используя вычисленный ключ после атак перебором | |
| 26 | Разрыв процедуры аутентификации, вызванный созданными задержками | |

## 3. Анализ уязвимостей аутентификации сетей сотовой связи 3G

Активное распространение сетей сотовой связи 3G началось в 2000-х годах. Так в 2001 году крупнейший японский оператор связи NTT DoCoMo запустил первую коммерческую сеть 3G, что стало важной вехой в развитии телекоммуникаций [44]. Основными стандартами 3G являются UMTS и CDMA2000. Они работают на основе технологии множественного доступа с кодовым разделением каналов (Code Division Multiple Access, CDMA). Среди этих стандартов наибольшее распространение получил UMTS. Рассмотрим его.

Архитектура сети UMTS претерпела значительные изменения, внедрив множество новых компонентов и улучшив существующие. В процедуре аутентификации сети UMTS используются следующие компоненты: пользователь-

ское устройство (User Equipment, UE), базовая станция (NodeB), коммутатор мобильных сетей (Mobile Switching Center, MSC), контроллер сети (Radio Network Controller, RNC), визитный регистр местоположения VLR с узлом обслуживания абонентов пакетной сети передачи данных (Serving GPRS Support Node, SGSN) и домашний регистр местоположения HLR с центром аутентификаций AuC. Т.е. термин «мобильная станция» в UMTS заменен на UE, акцентируя возможность использования в новых стандартах не только телефонов, но и смартфонов, планшетов, ноутбуков и иных персональных компьютеров.

На смену старому типу базовых станций, применяемых в предыдущих стандартах связи, появился новый тип – NodeB, в котором внедрен механизм Cell Breathing, позволяющий перегруженной соте передавать трафик абонентов соседним сотам, изменяя географический размер своей зоны обслуживания [45]. Введение в радиосеть RNC представляет собой еще одно значительное изменение в сетях UMTS. Этот новый контроллер отвечает за эффективное распределение ресурсов между станциями NodeB. Остальные элементы сети GSM, такие как MSC, VLR и HLR, в UMTS сохранили свою функциональность.

Появление новых стандартов сотовой связи предоставляет не только новые возможности для абонентов сети, но и новые методы безопасности, учитывая уязвимости предыдущих поколений сетей сотовой связи. Для исключения атаки «человек посередине», которая эксплуатировала уязвимости в сетях 2G, в сетях 3G появились функции аутентификации базовых станций, к которым подключается абонент сети. Алгоритм шифрования A5/1, используемый в сетях GSM, заменен на более криптостойкий блочный алгоритм KASUMI, использующий 64-битный размер блока и 128-битный ключ. Кроме параметра *RES* и ключа шифрования данных (Ciphering Key, $C_K$) в сетях 3G появился ключ целостности (Integrity Key, $I_K$) [46]. Он необходим для пометки сигнальных сообщений хэшем, вычисленным из самого сообщения и этого ключа целостности.

**Процедура аутентификации сетей сотовой связи стандарта UMTS** состоит из следующих шестнадцати этапов (см. рис. 11) [46].

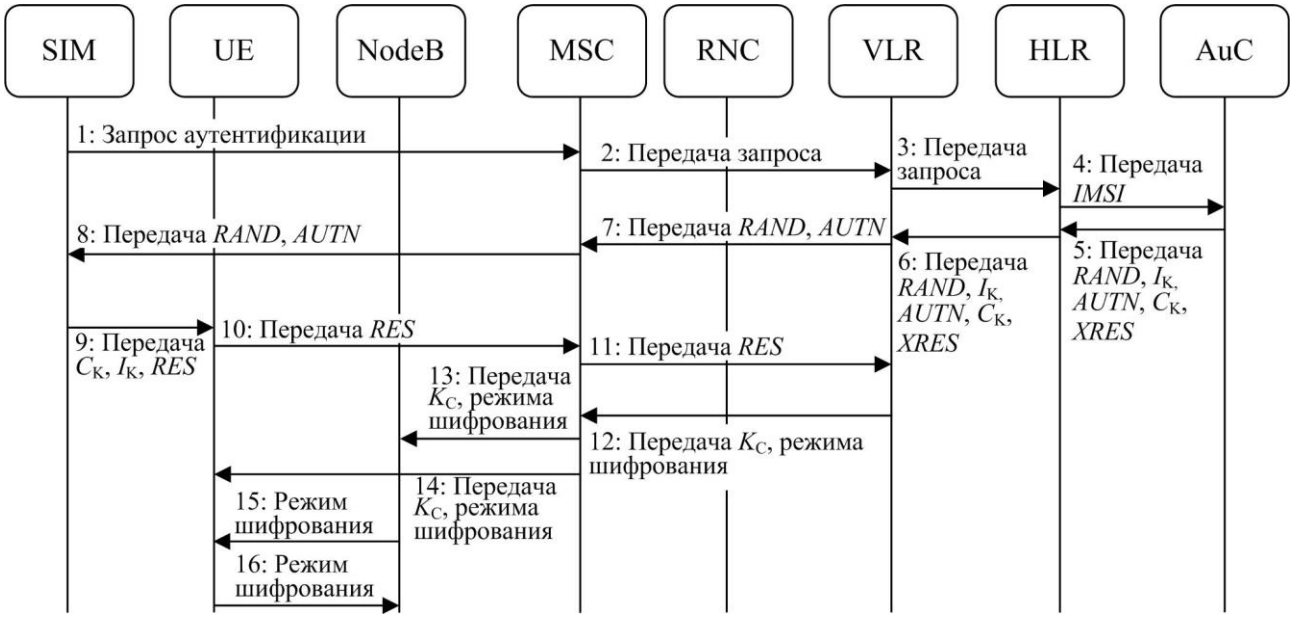


Рис. 11. Процедура аутентификации сетей UMTS

Этап 1. Процедура аутентификации пользовательского устройства (т.е. UE) активируется, отправляя сообщение в сеть (например, во время процесса обновления местоположения UE) [47].

Этап 2. После получения сообщения от UE коммутатор мобильных сетей (т.е. MSC) инициирует соответствующий процесс с гостевым регистром местоположения VLR.

Этап 3. VLR принимает решение об аутентификации UE и отправляет запрос на аутентификацию в HLR, включающий в себя *IMSI* абонента.

Этап 4. HLR, используя полученный *IMSI*, запрашивает у центра аутентификации (т.е. AuC) векторы аутентификации (Authentication vector, AV).

Этап 5. На основе полученного *IMSI* AuC использует индивидуальный ключ *K* (аналогично $K_i$ в GSM) и генерирует порядковый номер аутентификации (Sequence number, SQN), который должен быть больше любого раннее сгенерированного значения для данного пользовательского оборудования. Для каждого запрошенного вектора аутентификации AV в AuC также генерируется случайное значение *RAND*, необходимое для выполнения пяти следующих функций (см. рис. 12) [46]:

- функции *f*1 для создания значения кода аутентификации сообщения *MAC* (Message Authentication Code);
- функции *f*2 для создания значения ожидаемого ответа сети *XRES*;
- функции *f*3 для создания значения ключа шифрования $C_K$;
- функции *f*4 для создания значения ключа целостности $I_K$;
- функции *f*5 для создания значения ключа анонимности $A_K$.

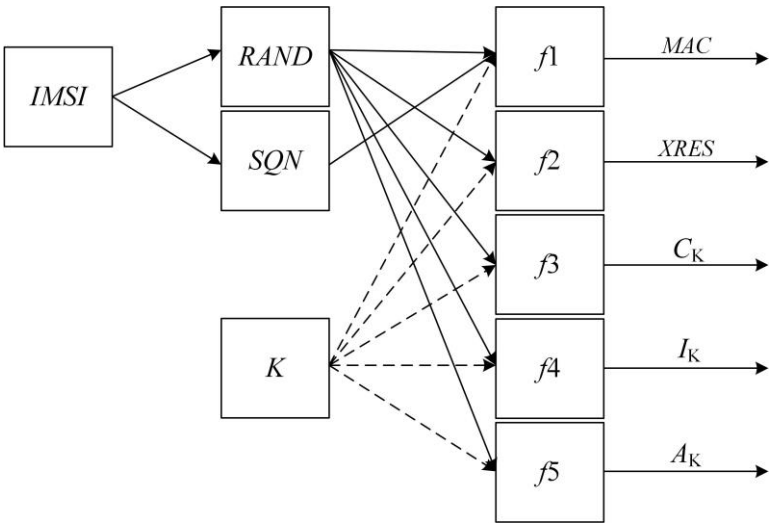


Рис. 12. Генерация вектора аутентификации

Далее создается ключ аутентификации (Authentication Token, AUTN) в результате конкатенации обфусцированной (преобразованной для затруднения анализа) последовательности *SQN*, $A_K$, AMF (Access and Mobility Management Function) и *MAC*. *AMF* – это 16-битное значение, которое используется как в UE, так и в сети. Оно содержит информацию, необходимую для выполнения аутентификации и управления безопасностью. После этого AuC возвращает в HLR массив значений (*RAND*, *AUTN*, $C_K$, $I_K$, *XRES*).

Этап 6. HLR передает *RAND*, *AUTN*, $C_K$, $I_K$ и *XRES* в VLR. VLR сохраняет $C_K$, $I_K$ и *XRES* для последующего использования.

Этап 7. VLR запрашивает аутентификацию абонента у MSC, пересылая значения *RAND* и *AUTN*.

Этап 8. MSC пересылает на UE запрос аутентификации со значениями *RAND* и *AUTN*.

Этап 9. UE запускает процесс AUTHENTICATE на SIM-карте, используя значения *RAND* и *AUTN*. SIM-карта с использованием значений *RAND*, *AMF* (вычисляется на основе *AUTN*), *SQN* и *K* выполняет функции *f*1, *f*2, *f*3, *f*4 и *f*5, получая значения *MAC*, *RES*, $C_K$, $I_K$ и $A_K$. Далее вычисляются и проверяются значения $SQN \oplus A_K$ и *MAC* с полученными значениями из *AUTN*. Здесь и далее знак $\oplus$ обозначает логическую операцию исключающего ИЛИ (побитового сложения по модулю, XOR), результат выполнения которой истинен тогда и только тогда, когда один из аргументов истинен, а второй ложен. После этих вычислений SIM-карта передает UE сгенерированные значения $C_K$, $I_K$ и *RES*.

Этап 10. UE сохраняет полученные значения $C_K$ и $I_K$, вычисляя из них ключ шифрования $K_C$ для дальнейшего использования. UE отправляет ответ на запрос аутентификации в MSC с вычисленным значением *RES*.

Этап 11. MSC отправляет в VLR значение *RES*, отправленное пользовательским устройством.

Этап 12. VLR сравнивает значения *RES* и *XRES*. Если значения равны, то SIM-карта аутентифицируется в сети. VLR получает $K_C$ из $C_K$ и $I_K$. Если значения не совпадают, то процедура завершается. В противном случае VLR отправляет сообщение для установления режима шифрования в MSC, которое предоставляет $K_C$ и выбранный алгоритм шифрования, поддерживаемый NodeB и UE. После этого сохраненный $K_C$ используется для шифрования всех данных, передаваемых между NodeB и UE абонента.

Этап 13. MSC отправляет запрос к NodeB и UE для начала шифрования, предоставив $K_C$ и выбранный алгоритм шифрования.

Этап 14. NodeB сохраняет ключ $K_C$ для дальнейшего использования и сообщает выбранный режим шифрования для UE.

Этап 15. UE, получив от NodeB информацию о выбранном режиме шифрования, включает шифрование передаваемых данных, используя сохраненный $K_C$ в качестве ключа шифрования, и отправляет обратно на NodeB информацию о режиме шифрования.

Этап 16. BTS начинает применение шифрования, используя сохраненный $K_C$, и передает информацию о режиме полного шифрования обратно в MSC.

После этого этапа процедура аутентификации завершается, и информация между NodeB и UE абонента шифруется.

Для процедуры аутентификации сетей сотовой связи третьего поколения ранее опубликованы следующие уязвимости.

1. О перехвате пользовательских данных, используя уязвимости в алгоритме шифрования, впервые сообщили **J. Tsay** и **S. F. Mjølsnes** в работе [48]. Алгоритм шифрования KASUMI, используемый в UMTS, имеет ряд обнаруженных уязвимостей, которые позволяют проводить криптоаналитические ата-

ки и получать пользовательские данные. В 2010 году израильские ученые **О. Данкельман**, **Н. Келлер** и **А. Шамир** продемонстрировали «атаку на связанных ключах» на алгоритм шифрования KASUMI (A5/3), используемый в сетях 3G. Эта атака позволяет получить 128-битный ключ с помощью одного компьютера менее чем за 2 часа [30]. В 2005 году в [49] **U. Meyer** и **S. Wetzel** продемонстрировали атаку на сеть UMTS через сеть GSM. В декабре 2014 году немецкий эксперт по безопасности сотовых сетей и основатель компании Security Research Labs **К. Нол** на ежегодной конференции 31C3 выступил с докладом на тему атаки по боковому каналу в сетях 3G, используя уязвимость в сигнальном протоколе SS7 (*Signalling System 7*) [50].

2. В работе [51] **R. Borgaonkar**, **L. Hirschi**, **S. Park** и **A. Shaik** показали, что при выполнении запроса на подключение злоумышленник также может перехватить, модифицировать или заблокировать передачу *IMSI* для последующих атак IMSI-paging и IMSI-probing. Используя эти значения, также возможны DoS- и DDoS-атаки на элементы обслуживающей сети с использованием как собранных, так и сгенерированных злоумышленником значений.

3. Атаки, использующие логическую уязвимость в механизме отказа AKA, связанную с применением операции побитового сложения по модулю (XOR), в ключе (токене) повторной синхронизации (Authentication Synchronization Token, AUTS) продемонстрировали **R. Borgaonkar**, **L. Hirschi**, **S. Park** и **A. Shaik** в той же работе [51]. *AUTS* создается в USIM для передачи информации о повторной синхронизации порядкового номера *SQN*. Он включает в себя два параметра: *CONC* (Concealed value) и *MAC*. Значение *CONC* представляет собой:

$$CONC = SQN_{\text{UE}} \oplus A_{\text{K}}, \quad (4)$$

где: *CONC* – это зашифрованное значение порядкового номера $SQN_{\text{UE}}$, используемое в *AUTS*. Оно отправляется в сеть для того, чтобы скрыть реальный порядковый номер $SQN_{\text{UE}}$ от злоумышленников; $A_{\text{K}}$ – это ключ анонимности, вычисляемый с помощью криптографической функции *f*5, которая использует секретный ключ аутентификации устройства и случайное значение *RAND*.

Для реализации уязвимости злоумышленнику необходимо перехватить два разных *AUTS*, содержащие значения $CONC_1$ и $CONC_2$ в два разных момента времени $t_1$ и $t_2$, когда устройство пытается синхронизироваться с сетью. В момент времени $t_1$ UE создает ключ синхронизации с зашифрованным номером последовательности:

$$CONC_1 = SQN_{\text{UE1}} \oplus A_{\text{K}}, \quad (5)$$

где: $SQN_{\text{UE1}}$ – значение порядкового номера в момент $t_1$; $A_{\text{K}}$ – ключ, необходимый для скрытия значения $SQN_{\text{UE1}}$, вычисленный с помощью индивидуального ключа *K* и значения *RAND*.

В момент времени $t_2$ устройство снова проходит аутентификацию с тем же значением *RAND*, и ключ синхронизации содержит следующее значение:

$$CONC_2 = SQN_{\text{UE2}} \oplus A_{\text{K}}, \quad (6)$$

где: $SQN_{\text{UE2}}$ – значение порядкового номера в момент $t_2$; $A_{\text{K}}$ – такое же, как и в первом запросе, поскольку оно зависит от неизменного *RAND*.

Злоумышленник, перехватив оба значения $CONC_1$ и $CONC_2$, может их сложить по модулю, т.е. выполнить операцию XOR:

$$CONC_1 \oplus CONC_2 = SQN_{UE1} \oplus A_K \oplus SQN_{UE2} \oplus A_K. \quad (7)$$

Поскольку $A_K \oplus A_K = 0$ (т.е. применение операции XOR к двум одинаковым числам дает ноль), то выражение (7) упрощается до:

$$CONC_1 \oplus CONC_2 = SQN_{UE1} \oplus SQN_{UE2}. \quad (8)$$

Таким способом злоумышленник получает значение $SQN_{UE1} \oplus SQN_{UE2}$, то есть разницу между порядковыми номерами в двух разных временных точках. Зная разницу $SQN_{UE1} \oplus SQN_{UE2}$, злоумышленник может получить информацию о том, насколько изменился порядковый номер между двумя запросами аутентификации. Эта информация может быть использована для анализа частоты взаимодействия устройства с сетью, что нарушает конфиденциальность. В ряде случаев это может привести к атаке, если будут известны конкретные шаблоны обновления счетчиков устройства, а также предоставить косвенную информацию о действиях устройства. Таким образом, рассматриваемая уязвимость связана с тем, что операция XOR в ключе синхронизации *AUTS* позволяет извлечь информацию о порядковых номерах, если аутентификационный запрос использует одно и то же значение *RAND*.

4. Атака мониторинга активности. В работе [51] **R. Borgaonkar**, **L. Hirschi**, **S. Park** и **A. Shaik** рассмотрели уязвимость, позволяющую отследить активность абонента между двумя периодами времени. В этой атаке цель злоумышленника заключается в определении *n* младших значащих битов $SQN_{UE}$ в моменты времени $t_1$ и $t_2$. Используя разницу между значениями счетчиков, атакующий может вычислить «интенсивность активности» пользователя, например, продолжительность подключения к сети, количество звонков, SMS-сообщений. Это, в свою очередь, позволяет нарушить конфиденциальность данных о поведении абонента. Для выполнения атаки злоумышленник должен взаимодействовать как с UE, так и с сетью.

5. В стандарте UMTS также существует уязвимость, позволяющая создать рассинхронизацию порядковых номеров аутентификации (т.е. *SQN*), что может привести к серьезным нарушениям в работе сети [52]. Эта атака может быть проведена как с использованием имеющейся базы данных собранных значений, так и с использованием сгенерированных значений с указанием диапазона для проведения атаки, целью которой является нарушение работы абонентов конкретного оператора. Алгоритм атаки состоит из шести этапов (см. рис. 13).

Этап 1. UE инициирует запрос на аутентификацию.

Этап 2. Злоумышленник перехватывает в радиоканале запрос на аутентификацию от UE и имитирует это оборудование путем отправки в сеть *N* запросов аутентификации с такими же параметрами. Количество запросов *N* должно превышать допустимую разность $SQN_i$ и $SQN_{i-1}$ (по умолчанию 2).

Этап 3. VLR запрашивает у HLR и получает от него *N* векторов аутентификации: $AV_1$ (для $SQN_1$), $AV_2$ (для $SQN_2$) … $AV_N$ (для $SQN_N$). VLR пересылает UE значения этих векторов, которые перехватывает устройство злоумышленника, не давая их получить UE.


Рис. 13. Процедура рассинхронизации порядковых номеров аутентификации

Этап 4. Злоумышленник перехватывает значения векторов аутентификации по радиоканалу и передает на UE ровно такое количество векторов, при котором разница между *SQN* на устройстве пользователя и у сети превысила допустимую разницу, установленную в сети (по умолчанию 2). Таким образом, злоумышленник формирует условия для возникновения рассинхронизации между устройством пользователя и сетью.

Этап 5. UE инициирует новую процедуру аутентификации и запрашивает новый вектор аутентификации у сети.

Этап 6. Сеть создает новый вектор аутентификации и передает его UE. Поскольку злоумышленник ранее передал UE часть векторов, разница между *SQN* на стороне сети и *SQN* на устройстве становится больше допустимой. Это приводит к рассинхронизации.

Например, злоумышленник передал на UE один вектор аутентификации $AV_1$ ($SQN_1$), а остальные векторы $AV_2$ ($SQN_2$), $AV_3$ ($SQN_3$) и $AV_4$ ($SQN_4$) перехватил. В результате на стороне UE остается последняя известная последовательность $SQN_1$, в то время как в сети текущая последовательность уже обновлена до $SQN_4$. Разница между $SQN_4$ и $SQN_1$ составляет 3, что превышает допустимое значение (по умолчанию 2). UE обнаруживает, что $SQN_2 < SQN_4$ и отклоняет аутентификацию с ошибкой синхронизации.

6. Перехват пользовательских данных, используя принудительное понижение используемого стандарта сотовой связи. Данная уязвимость основана на реакции сети при радиоподавлении сигнала 3G сетей и перенаправления на частоты сетей GSM для дальнейшего перехвата данных. Немецкая компания PKI Electronic Intelligence производит IMSI-перехватчики для сетей как 2G, так и для 3G и 4G, принцип работы которых основан на использовании этой уязвимости сети [53]. Такие устройства могут перехватывать пользовательские идентификаторы (*IMSI, TMSI* и *IMEI*) и управляться с ноутбука, планшета или смартфона (см. рис. 14). Функционал таких устройств позволяет блокировать определенный перечень UE и создавать «белый список» абонентов, которым разрешен доступ в сеть. Кроме того, израильская компания Septier, предоставляющая решения и продукты для разведывательных и правоохранительных служб, разработала мини-перехватчик для сетей 2G и 3G, позволяющий хранить его в кармане одежды (см. рис. 15) [54]. Функционал устройства позволяет извлекать *IMSI* цели и определять ее местоположение.


Рис. 14. IMSI-перехватчик PKI 1625

Рис. 15. Портативный IMSI-перехватчик для сетей 3G

7. В работе [51] **R. Borgaonkar**, **L. Hirschi**, **S. Park** и **A. Shaik** предложили атаку, использующую уязвимость в механизме обработки ошибок в процессе аутентификации. В начале злоумышленник наблюдает за сеансом аутентификации целевого пользователя и записывает запрос сети к его UE, содержащий *RAND* и *AUTN*. Затем, когда злоумышленник хочет проверить, принадлежит ли другой сеанс тому же целевому пользователю, он воспроизводит записанный запрос и анализирует тип полученного сообщения об ошибке. Если перехвачено специальное сообщение Sync Failure (ошибка синхронизации), то это означает, что сеанс принадлежит тому же пользователю, за которым следит злоумышленник. Если перехвачено специальное сообщение MAC Failure (ошибка аутентификации), то сеанс принадлежит другому пользователю. Такая атака не требует выполнения сложных вычислений, а результаты однозначны, что делает её эффективной для отслеживания пользователей.

Кроме известных уязвимостей в ходе настоящего исследования с использованием метода генерации кибератак на телекоммуникационное оборудование выявлены следующие уязвимости сетей сотовой связи третьего поколения.

1. Аналогично уязвимости в GSM злоумышленник может вести мониторинг абонентов сети, которые совершают запросы аутентификации, и сохранять эти запросы в собственную базу данных. Повторной успешной аутентификацией возможно вызвать перераспределение *TMSI*. Кроме того, сохранилась возможность проверки наличия в базе данных конкретного значения *IMSI* на основе полученных ответов от сети.

2. При передаче *RAND* и *AUTN* отсутствует контроль целостности и существует уязвимость, позволяющая перехватить, модифицировать и отправить собственные значения *RAND* и *AUTN* на UE, вызвав сбой в аутентификации или неправильное вычисление значения *RES*.

3. Прямой доступ к *SQN*. Если злоумышленник может получить доступ к *SQN* пользовательского устройства, то он способен предсказать значения *SQN* в будущем. Это снижает эффективность защиты от атак, основанных на повторном использовании запросов, и делает протокол уязвимым к дальнейшей компрометации.

4. Повторное использование $RES_i$ и процедуры восстановления сбоя синхронизации. Эта уязвимость может быть использована следующим способом.

Этап 1. Злоумышленник проводит атаку для сбоя синхронизации в сети.

Этап 2. UE отправляет в сеть запрос об ошибке синхронизации. Это сообщение перехватывает злоумышленник, записывает и пересылает в сеть.

Этап 3. Сеть, получив такое сообщение, отсылает новые значения *RAND* и *AUTN* в UE.

Этап 4. UE после вычисления ответа *RES* отправляет его в сеть. Злоумышленник перехватывает это сообщение, записывает и отправляет его в сеть.

Зная, что $RES_i$ и $AUTS_i$ принадлежат одному аутентификационному сеансу, злоумышленник может успешно пройти проверку сравнения *RES* с *XRES*, даже если после перехвата этих значений уже прошло достаточно времени. Такая уязвимость позволяет регистрировать абонента в разных географических зонах и разрывать установленные соединения, назначая новый *TMSI*.

5. Аналогично сетям GSM при перехвате и задержке данных, передаваемых по сети, злоумышленник может привести к истечению времени таймера аутентификации, что приведет к завершению процедуры аутентификации, нарушая нормальный процесс установления безопасного соединения.

Последствия этих угроз могут быть следующими:

1) снижение скорости или полное отсутствие доступа к сети оператора;
2) ошибки приложений, требующих постоянного соединения с Интернет;
3) недоступность экстренных звонков;
4) отслеживание местоположения абонента;
5) повышение расходов на техническую поддержку и выявление проблемы операторами сотовой связи;
6) репутационные риски для оператора;
7) повышение потребления аккумулятора UE из-за постоянной работы;
8) повышенное потребление ресурсов UE, необходимых для обработки поступающих запросов;
9) получение доступа к конфиденциальной информации абонента и оператора;
10) потеря данных при неудачной аутентификации в сети.

В таблице 2 перечислены уязвимости в процедуре аутентификации сетей стандарта UMTS.

## 4. Анализ уязвимостей аутентификации сетей сотовой связи 4G

В начале 2000-х годов стало ясно, что сети сотовой связи 3G, такие как UMTS и HSPA (High Speed Packet Access), уже не справляются с растущими потребностями пользователей в передаче данных. В 2004 году консорциум 3GPP (3rd Generation Partnership Project) начал работу над стандартами для сетей 4G [55]. В 2008 году опубликованы первые спецификации стандарта LTE, которые определяли основные технические требования к новым сетям. Эти технологии позволили эффективнее использовать доступный радиочастотный спектр и обеспечили высокие скорости передачи данных. В 2009 году началось коммерческое развертывание сетей LTE [55]. Одними из первых стран, внедривших LTE, стали Швеция и Норвегия, где компания TeliaSonera запустила сети LTE в Стокгольме и Осло [56]. К середине 2010-х годов стандарт LTE стал доступен в большинстве крупных городов мира. С развитием технологии по-

явились усовершенствования и новые версии стандарта LTE. Самые известные из них – LTE Advanced (Release 10) и LTE Advanced Pro (Release 13) [57]. Сейчас сети LTE продолжают развиваться и использоваться в большинстве стран мира. Они обеспечивают базу для многих современных мобильных услуг, включая VoLTE (Voice over LTE) для высококачественных голосовых вызовов и IoT (Internet of Things) для подключения множества UE.

Таблица 2 – Уязвимости в процедуре аутентификации сетей UMTS

| № | Уязвимость | Публикации |
|---|---|---|
| 1 | Уязвимости в алгоритмах шифрования, используемых в процедуре аутентификации | [28, 29, 30, 48, 49, 50] |
| 2 | Рассинхронизация порядковых номеров аутентификации *SQN* | [52] |
| 3 | Изменение содержимого запроса аутентификации от UE к NodeB | [51] |
| 4 | Блокирование запроса аутентификации от UE к NodeB | |
| 5 | Вскрытие идентификатора *IMSI* абонента | |
| 6 | DoS-атаки и DDoS-атаки на элементы сети | |
| 7 | Определение наличия абонента по полученному ответу обработки ошибки | |
| 8 | Уязвимость в механизме AKA, основанная на использовании XOR в ключе повторной синхронизации *AUTS* | |
| 9 | Определение активности абонента на основе полученных *SQN* | |
| 10 | Атака на понижение – меняет аутентификацию UMTS на GSM | [41, 52] |
| 11 | Мониторинг подключающихся абонентов к сети | Рассматриваются впервые |
| 12 | Переназначение TMSI на основании нового запроса | |
| 13 | Проверка наличия *IMSI* в базе на основе полученных ответов | |
| 14 | DoS-атаки и DDoS-атаки на UE, используя значения *RAND, AUTN* | |
| 15 | Перехват и модификация значений *RAND, AUTN* | |
| 16 | Блокировка передачи *RAND, AUTN* | |
| 17 | Отсутствие контроля целостности значения *RAND* | |
| 18 | Передача собственных значений *RAND, AUTN* | |
| 19 | Предсказание последующих *SQN* при прямом доступе | |
| 20 | Повторное использование $RES_i$ и процедуры восстановления синхронизации после сбоя | |

В сетях 4G стали использоваться новые алгоритмы шифрования 128-EEA1 и 128-EEA2, основанные на AES и SNOW36, которые пришли на замену алгоритму KASUMI. Новые алгоритмы имеют высокую криптостойкость, гибкость и позволяют работать с высокоскоростными сетями, оказывая минимальное влияние на производительность системы. В работе процедуры аутентификации в стандарте LTE задействованы следующие элементы сети [58]:

1) UE: пользовательское устройство, которое содержит SIM-карту. SIM-карта содержит *IMSI* и индивидуальный ключ пользователя *K*;
2) HSS (Home Subscriber Server): центральная база данных, содержащая информацию об абонентах сети (их *IMSI* и индивидуальный ключ пользователя *K*). Она генерирует аутентификационные векторы, используя *K* и случайные значение *RAND*, и отправляет их в MME;
3) MME (Mobility Management Entity): ключевой элемент сети LTE, ответственный за управление мобильностью и сессиями. Он инициирует

аутентификационные процедуры, отправляя запросы к HSS и получая аутентификационные векторы;

4) eNodeB (evolved Node B): базовая станция, обеспечивающая радиосвязь между UE и элементами сети. eNodeB передает аутентификационные запросы между UE и MME.

**Процедура аутентификации сетей сотовой связи стандарта LTE** состоит из следующих десяти этапов (см. рис. 16) [58].

Этап 1. UE делает запрос к MME через eNodeB.

Этап 2. MME запрашивает аутентификационные данные, относящиеся к конкретному *IMSI*, отправляя запрос аутентификации к AuC через HSS.

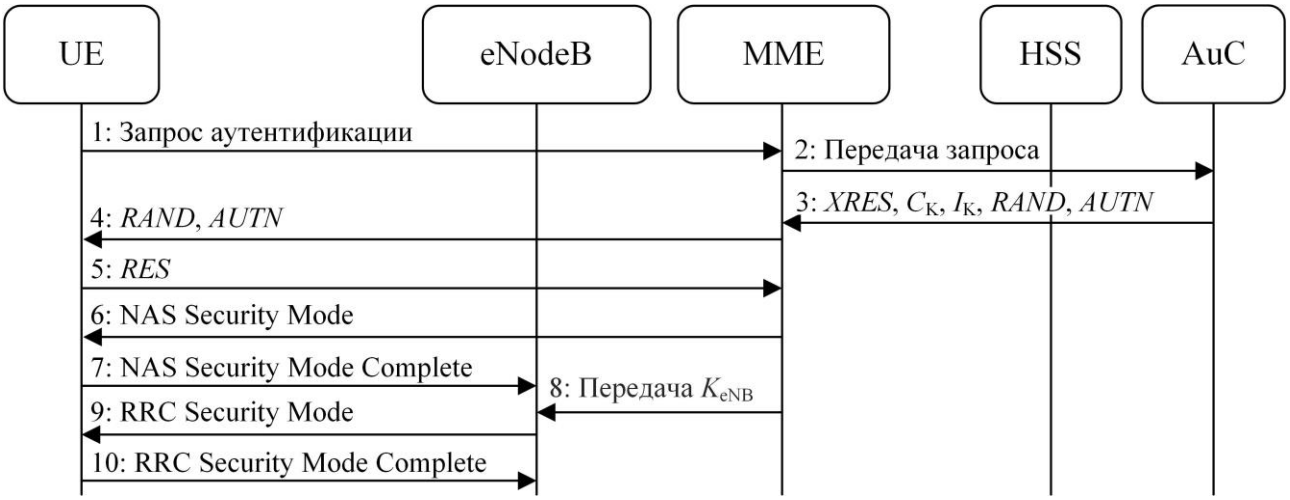


Рис. 16. Процедура аутентификации в сети LTE

Этап 3. AuC находит индивидуальный ключ, относящийся к конкретному *IMSI* и вычисляет аутентификационные данные. AuC через HSS отправляет обратно вектор аутентификации в MME.

Этап 4. MME получает значения $I_K$, $C_K$, *XRES*, *RAND* и *AUTN* от AuC и отправляет *AUTN* и *RAND* в UE.

Этап 5. UE вычисляет $I_K$, $C_K$, *RES* и *XMAC* (ожидаемое значение *MAC*) с помощью своего индивидуального ключа *K* и полученных значений *AUTN* и *RAND*. После чего он отправляет *RES* в MME.

Этап 6. MME после получения значения *RES* от UE сравнивает его с собственным значением *XRES* и, если они совпадают, то аутентификация прошла успешно. В противном случае MME отправляет сообщение о сбое аутентификации (Authentication failure) в UE. После успешной аутентификации вычисляются значения ключей $K_{ASME}$, $K_{eNB}$, $K_{nas\text{-}int}$ и $K_{nas\text{-}enc}$ (см. таблицу 3). Далее MME отправляет NAS Security Mode Command в UE.

Этап 7. UE вычисляет $K_{ASME}$, $K_{eNB}$, $K_{nas\text{-}int}$, $K_{nas\text{-}enc}$ и отправляет сообщение NAS Security Mode Complete в MME.

Этап 8. MME отправляет $K_{eNB}$ в eNodeB.

Этап 9. eNobeB вычисляет значения $K_{rrc\text{-}int}$, $K_{rrc\text{-}enc}$, $K_{up\text{-}enc}$ и отправляет сообщение RRC Security Mode в UE.

Этап 10. UE вычисляет $K_{rrc\text{-}int}$, $K_{rrc\text{-}enc}$, $K_{up\text{-}enc}$ и отправляет в MME сообщение RRC Security Mode Complete.

Таблица 3 – Ключи безопасности в процедуре аутентификации сети LTE

| Ключ | Предназначение | Генерация |
|---|---|---|
| $K_{ASME}$ (Key for Access Security Management Entity) | Основной ключ для защиты управления и передачи данных между MME и UE. Используется для генерации других ключей | Генерируется из $C_K$ и $I_K$ с использованием шифрования |
| $K_{eNB}$ (Key for eNodeB) | Ключ для защиты связи между UE и eNodeB. Используется для генерации ключей RRC | Генерируется из $K_{ASME}$ с использованием HMAC-SHA-256 и функции получения ключа KDF (Key Derivation Function) |
| $K_{nas\text{-}int}$ (Key for NAS Integrity Protection) | Ключ для обеспечения целостности NAS (Non-Access Stratum) сообщений между MME и UE | Генерируется из $K_{ASME}$ с использованием KDF |
| $K_{nas\text{-}enc}$ (Key for NAS Encryption) | Ключ для шифрования NAS сообщений между MME и UE | Генерируется из $K_{ASME}$ с использованием KDF |
| $K_{rrc\text{-}int}$ (Key for RRC Integrity Protection) | Ключ для обеспечения целостности RRC сообщений между eNodeB и UE | Генерируется из $K_{eNB}$ с использованием KDF |
| $K_{rrc\text{-}enc}$ (Key for RRC Encryption) | Ключ для шифрования RRC сообщений между eNodeB и UE | Генерируется из $K_{eNB}$ с использованием KDF |
| $K_{up\text{-}enc}$ (Key for User Plane Encryption) | Ключ для шифрования пользовательских данных (U-plane data) между eNodeB и UE | Генерируется из $K_{eNB}$ с использованием KDF |

После завершения процедуры все сообщения между UE и eNodeB будут надежно защищены и зашифрованы с использованием ключей $K_{rrc\text{-}int}$ и $K_{rrc\text{-}enc}$. Пользовательские данные, передаваемые через пользовательскую плоскость (User Plane), будут шифроваться только с использованием ключа $K_{up\text{-}enc}$.

Процедура аутентификации в LTE, несмотря на значительное повышение безопасности в сравнении с предыдущими поколениями, все еще подвержена уязвимостям. Эти уязвимости могут быть связаны с различными аспектами, начиная от возможности перехвата и анализа зашифрованного трафика до слабых мест в реализации криптографических протоколов и системы аутентификации. Рассмотрим опубликованные уязвимости.

1. Одним из основных векторов атак остаются IMSI-перехватчики, которые могут эмулировать базовые станции и заставлять UE подключаться к ним вместо официальных сетей операторов, передавая свои идентификационные значения. Это открывает возможности для различных атак, включая прослушивание, изменение передаваемых данных между UE и сетевыми элементами, отслеживание местоположения пользователей с помощью IMSI-paging и IMSI-probing. В 2014 году в газете News Tribune из Такомы, штат Вашингтон, опубликовано сообщение о том, что управление по борьбе с наркотиками (DEA) сделало заказ на «обновление StingRay II до Hailstorm» [59]. Согласно сообщению устройства Hailstorm предоставляют возможность устройствам StingRay перехватывать телефоны, работающие в сетях LTE даже после того, как использование сетей 2G было прекращено. Это означает, что искоренение стан-

дартов GSM не делает устаревшим использование перехватчиков. Компания Martone Radio Technology также рекламирует продукты, способные перехватывать телефоны, использующие сети LTE [60]. Однако возможно, что это подразумевает способность блокировать сигналы 4G и принудительно переключать телефоны на соединение 2G перед проведением атаки «человек посередине».

2. В стандарте LTE присутствуют наследственные уязвимости от прошлых поколений: возможность перехвата, модификации и блокирования запросов, осуществление DoS-атак и DDoS-атак на UE и элементы сети, рассинхронизация порядковых номеров аутентификации *SQN*, перехват, модификация и блокировка значений *RAND* и *AUTN*, определение наличия абонента по полученному ответу обработки ошибки, уязвимость в механизме AKA, основанная на использовании XOR в ключе повторной синхронизации *AUTS*, определение активности абонента на основе полученных *SQN*, предсказание последующих *SQN* при прямом доступе, повторное использование *i*-го значения $RES_i$ и процедуры восстановления сбоя синхронизации.

3. В сетях 4G появились новые идентификаторы *GUTI, SUCI* и *SUPI*. Однако их можно перехватить, модифицировать и заблокировать их передачу. В 4G также сохранилась уязвимость предыдущих поколений, связанная с перехватом личных идентификаторов. Эти атаки возможно проводить с помощью широко распространенных программно-определяемых систем с использованием программы srsUE [61]. В спецификации 3GPP TR 33.899 [62] такие атаки выделены как ключевая проблема. В связи с серьезностью угрозы утечки *SUPI* 3GPP особое внимание уделяет защите от нее в 5G Release 15, о чем свидетельствует п. 5.2.5 спецификации TS 33.501 [63].

4. Временные идентификаторы пользователя, которые используются для уменьшения вероятности обнаружения и отслеживания определенного пользователя в сети, на практике могут оставаться на длительный период времени за определенным абонентом [64, 65].

5. Для защиты *SUPI* используется криптографическая схема ECIES (Elliptic Curve Integrated Encryption Scheme), основанная на эллиптических кривых. Публичный ключ для шифрования *SUPI* хранится в защищенной памяти USIM-карты, а закрытый ключ в SIDF (Subscription Identifier De-concealing Function, см. далее архитектуру 5G). Однако если злоумышленник обладает квантовым компьютером, то он может решить эту задачу с помощью квантового алгоритма **П. Шора** [66, 67].

6. В работе [51] **R. Borgaonkar**, **L. Hirschi**, **S. Park** и **A. Shaik** показали, что постоянный идентификатор подписки абонента *SUPI* содержит мобильный код страны и мобильный код сети, которые не шифруются при передаче, что позволяет злоумышленнику идентифицировать принадлежность подключаемых абонентов к определенной стране и оператору.

7. В той же статье [51] **R. Borgaonkar**, **L. Hirschi**, **S. Park** и **A. Shaik** рассмотрели атаки перебора *SUPI*: злоумышленник может выбрать произвольный *SUPI* и отправить соответствующий зашифрованный *SUCI* в сеть. Получая ответы сети (запрос аутентификации или сообщение об ошибке), он может определить его присутствие или отсутствие в базе данных сети. Изменение получа-

емого ответа позволит злоумышленнику подтвердить или опровергнуть нахождение абонента в данной соте.

Кроме известных уязвимостей в ходе настоящего исследования с использованием метода генерации кибератак на телекоммуникационное оборудование установлено, что в сетях сотовой связи четвертого поколения могут также в полном объеме существовать уязвимости, характеристика которых приведена в предыдущем разделе настоящей статьи. Однако следует отметить, что с появлением новых идентификаторов пользователей уязвимости, связанные с переназначением *TMSI* и проверкой их наличия в базе данных оператора (пп. 12, 13 в таблице 2), стали неактуальны. С учетом этого уязвимости процедуры аутентификации сетей стандарта LTE перечислены в таблице 4.

Таблица 4 – Уязвимости процедуры аутентификации сетей стандарта LTE

| № | Уязвимость | Публикации |
|---|---|---|
| 1. | Изменение содержимого запроса аутентификации от UE к eNodeB | [51, 61] |
| 2. | Блокирование запроса аутентификации от UE к eNodeB | [51] |
| 3. | DoS-атака и DDoS-атаки на элементы сети | |
| 4. | Определение наличия абонента по полученному ответу обработки ошибки | |
| 5. | Уязвимость в механизме AKA, основанная на использовании XOR в ключе повторной синхронизации *AUTS* | |
| 6. | Определение активности абонента на основе полученных *SQN* | |
| 7. | Определение MNC и MCC по *SUPI* абонента | |
| 8. | Вскрытие идентификатора *SUPI* абонента | [66, 67] |
| 9. | Рассинхронизация порядковых номеров аутентификации *SQN* | [52] |
| 10. | Атака на понижение меняет аутентификацию LTE на GSM | [41, 52] |
| 11. | Временные идентификаторы с длительным сроком действия | [64, 65] |
| 12. | Мониторинг подключающихся абонентов к сети | Рассматриваются впервые |
| 13. | DoS-атаки и DDoS-атаки на UE, используя значения *RAND, AUTN* | |
| 14. | Перехват и модификация значений *RAND, AUTN* | |
| 15. | Блокировка передачи *RAND, AUTN* | |
| 16. | Отсутствие контроля целостности значения *RAND* | |
| 17. | Передача собственных значений *RAND, AUTN* | |
| 18. | Предсказание последующих *SQN* при прямом доступе | |
| 19. | Повторное использование $RES_i$ и процедуры восстановления синхронизации после сбоя | |

## 5. Анализ уязвимостей аутентификации сетей сотовой связи 5G

В начале 2010-х годов Международный союз электросвязи (ITU) и консорциум 3rd Generation Partnership Project совместно с компаниями Ericsson, Nokia, Qualcomm, Huawei и Samsung вели работу по созданию и стандартизации сетей сотовой связи пятого поколения. С 2019 года в некоторых странах запущены первые коммерческие сети сотовой связи 5G. Но внедрение стандарта 5G столкнулось с проблемами, замедляющими процесс развертывания сетей нового поколения: дополнительные затраты на новое оборудование, его лицензирование и тестирование, согласование или освобождение частотного спектра.

В сетях 5G используется один из двух алгоритмов аутентификации: 5G-AKA, изначально разработанный для сетей 5G, или EAP-AKA, широко применяемый в современных беспроводных сетях (в первую очередь в сетях стандарта IEEE 802.11). Выбор используемого алгоритма зависит от решения мобильного оператора. В работе процедуры аутентификации в стандарте 5G задействованы следующие элементы сети [68]:

1) UE: пользовательское устройство, которое содержит SIM-карту. SIM-карта содержит *IMSI* и индивидуальный ключ пользователя $K_i$;
2) SEAF (Security Anchor Function): устройство, реализующее т.н. «якорную» функцию безопасности, отвечающее за аутентификацию пользовательского устройства при его регистрации в сети;
3) AUSF (Authentication Server Function): сервер аутентификации, принимающий запросы от SEAF и передающий их в ARPF;
4) ARPF (Authentication Credential Repository and Processing Function): база учетных данных аутентификации, которая хранит индивидуальные ключи $K_i$ и криптографические параметры. Она обеспечивает генерацию векторов аутентификации для алгоритмов 5G-AKA и EAP-AKA;
5) UDM (Unified Data Management): устройство, реализующее унифицированную функцию данных. Основными услугами являются управление доступом и мобильностью, управление сеансами, короткие сообщения и обеспечение работы сервера аутентификации;
6) SIDF: устройство, реализующее функцию извлечения идентификатора пользователя, предназначенную для преобразования скрытого идентификатора пользователя *SUCI* в постоянный идентификатор *SUPI* во время процедуры аутентификации.

ARPF, UDM и SIDF обычно размещаются совместно в центрах данных оператора связи. Поэтому для них используют аббревиатуру ARPF/UDM/SIDF.

**Процедура аутентификации сетей сотовой связи стандарта 5G** состоит из следующих одиннадцати этапов (см. рис. 17) [63].

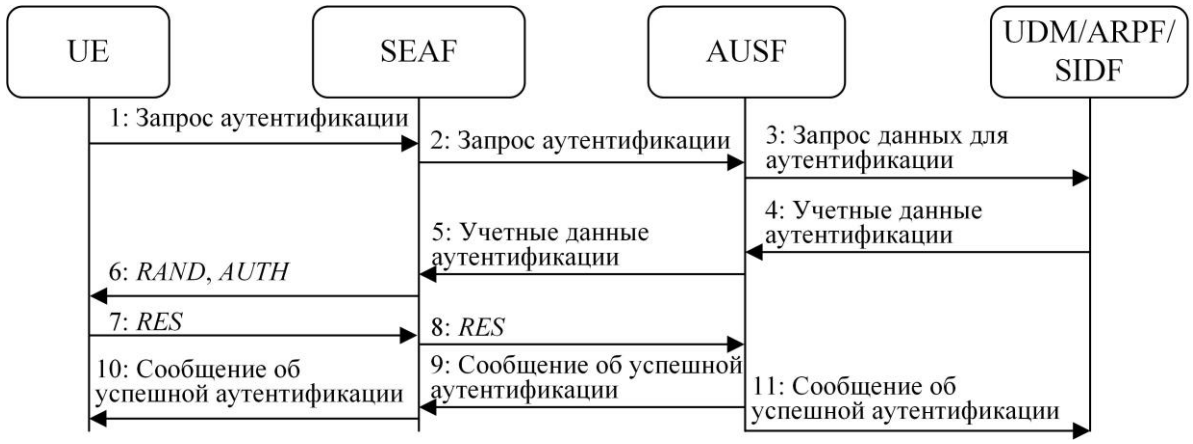


Рис. 17. Процедура аутентификации сетей 5G

Этап 1. UE посылает запрос аутентификации в SEAF. После получения от UE сообщения аутентификации SEAF инициирует процесс аутентификации. Одновременно с запросом UE отправляет SEAF временный идентификатор

*5G-GUTI* (Globally Unique Temporary Identifier) или зашифрованный идентификатор *SUCI* в случае, если *GUTI* еще не был выделен.

Этап 2. SEAF передает запрос в AUSF, который включает в себя: имя обслуживающей сети *SNN* (Serving Network Name), *SUPI* (если доступен и 5G-GUTI действителен) или *SUCI*.

Этап 3. AUSF проверяет, авторизована ли сеть для использования данного *SNN*. Если сеть не авторизована, то AUSF возвращает ошибку аутентификации. В противном случае AUSF отправляет запрос на получение данных для аутентификации в AUSF.

Этап 4. AUSF направляет запрос SIDF, который расшифровывает *SUPI* из *SUCI*. SIDF отправляет извлеченный *SUPI* в UDM, который в свою очередь ассоциирует *SUPI* с учетной записью абонента. После этого на основе полученных данных ARPF вычисляет вектор аутентификации, содержащий значения: *RAND*, *AUTN*, *XRES*, $C_K$ и $I_K$. Далее в зависимости от выбранного алгоритма вычисляются следующие необходимые значения:

– для алгоритма 5G-AKA: UDM/ARPF вычисляет ключ $K_{AUSF}$ из $C_K$, $I_K$ и *SNN*. Далее генерируется новый вектор аутентификации 5G (Home Environment Authentication Vector, HEAV), который содержит *RAND*, *AUTN*, *XRES*, $K_{AUSF}$. Эти значения отправляются в AUSF с пометкой о том, что их следует использовать исключительно для 5G-AKA;
– для алгоритма EAP-AKA: UDM/ARPF вычисляет значения $C_K'$ и $I_K'$ из полученных $C_K$, $I_K$ и *SNN* и составляет новый вектор аутентификации AV′, состоящий из *RAND*, *AUTN*, *XRES*, $C_K'$ и $I_K'$. После этого отправляет данные в AUSF с указанием использовать только EAP-AKA.

Этап 5. После получения вектора аутентификации AUSF вычисляет $K_{SEAF}$ (Key for SEAF) из полученного $K_{AUSF}$ и передает в SEAF сообщение, содержащее $K_{SEAF}$, *AUTN* и *RAND*. Если используется алгоритм 5G-AKA, то также передается ожидаемый ответ *HXRES* (Hashed Expected Response), вычисленный в результате хеширования полученного значения параметра *XRES*.

Этап 6. SEAF передает сообщение в UE, содержащее *RAND* и *AUTN*.

Этап 7. UE в случае использования алгоритма EAP-AKA, используя свой ключ (из USIM) и полученные значения *RAND* и *AUTN*, вычисляет *RES*. В случае использования алгоритма 5G-AKA дополнительно вычисляется *RES** из *RES*. Полученные значения UE отправляет в ответ SEAF.

Этап 8. SEAF пересылает значения в AUSF. В случае использования алгоритма 5G-AKA вычисляет значение *HRES** из полученного *RES** и сравнивает его с *HXRES*. Если значения совпадают, то SEAF считает аутентификацию успешной и отправляет сообщение об успешной аутентификации с полученным *RES** в AUSF.

Этап 9. AUSF сравнивает полученное значение с сохраненным и, если они одинаковы, AUSF считает сообщение об успешной аутентификации проверенным и сообщает об этом SEAF.

Этап 10. SEAF отправляет сообщение об успешной аутентификации в UE.

Этап 11. AUSF и UDM получают подтверждение, что UE аутентифицирован.

В сотовых системах 5G значительно улучшен вопрос безопасности и исключены многие уязвимости прошлых поколений: неаутентифицированный запрос IMEI, неизменность *GUTI*, связь между *GUTI* и *MSISDN* (это номер абонента в сети, соответствующий конкретному *IMSI* в HLR), устранена уязвимость, эксплуатируемая в атаке IMSI-paging. Остальные уязвимости аутентификации стандарт 5G наследовал от прошлых поколений, в том числе характерные для 4G ранее не опубликованные уязвимости.

Кроме того, в статье [69] **H. Khan** и **K. Martin** описана уязвимость, направленная на нарушение конфиденциальности местоположения абонента. Эта уязвимость позволяет установить, находится ли конкретное UE в определенном месте. Атака происходит по следующему сценарию.

Этап 1. Злоумышленник отслеживает сеанс 5G-AKA целевого пользователя $UE_x$ и извлекает соответствующее значение $CONC_x$, воспроизводя перехваченный запрос аутентификации для этого пользователя.

Этап 2. Спустя некоторое время, если злоумышленник хочет проверить, принадлежит ли другой неизвестный сеанс 5G-AKA пользователю $UE_x$, он снова направляет перехваченный запрос тому же пользователю и получает новое значение $CONC_y$.

Этап 3. В случае, если $CONC_x \approx CONC_y$, то закон распределения суммы $CONC_x \oplus CONC_y$ будет иметь схожую форму, и злоумышленник с определенной значительной вероятностью может определить, является ли новый пользователь $UE_y$ тем же, что и $UE_x$.

Кроме известных уязвимостей в ходе настоящего исследования с использованием метода генерации кибератак на телекоммуникационное оборудование выявлены также следующие уязвимости сетей сотовой связи пятого поколения.

1. Вычисление *SUPI* методом перебора. Для этого злоумышленнику необходимо дождаться, когда пользователь делает запрос, используя *SUCI* или *GUTI*, и перехватить ответ от сети со значениями *RAND* и *AUTN*. Далее злоумышленник блокирует запрос и дожидается истечения времени таймера аутентификации, чтобы при повторном запросе значение *AUTN* не изменилось. После этого он делает запросы к сети, используя сгенерированные значения *SUPI*, и получает ответы от нее. Данные действия повторяются до тех пор, пока в полученном ответе от сети не будет значения *AUTN*, равного значению *AUTN* при запросе легитимного абонента.

2. Во время проверки переданного значения *SNN* (см. этап 3 на рис. 17) может возникнуть ошибка аутентификации, которая завершает процедуру. Данную особенность может использовать злоумышленник для блокирования попыток подключения абонентов.

3. После вычисления значения *RES* устройство абонента ожидает ответа от сети. Злоумышленник также может отправить сообщение об ошибке аутентификации, тем самым завершив процедуру.

4. Кроме того, злоумышленник может прислать раньше сети сообщение об успешной аутентификации абоненту, а вычисленный ответ *RES* заблокировать на своем узле. Тем самым абонент не будет зарегистрирован в сети.

В таблице 5 перечислены уязвимости аутентификации сетей 5G.

Таблица 5 – Уязвимости процедуры аутентификации сетей 5G

| № | Уязвимость | Публикации |
|---|---|---|
| 1. | Атака на конфиденциальность местоположения абонента | [69] |
| 2. | Рассинхронизация порядковых номеров аутентификации *SQN* | [52] |
| 3. | Вскрытие идентификатора *SUPI* абонента | [66, 67] |
| 4. | DoS-атака и DDoS-атаки на элементы сети | [51] |
| 5. | Блокирование запроса аутентификации от UE к eNodeB | |
| 6. | Определение наличия абонента по полученному ответу обработки ошибки | |
| 7. | Уязвимость в механизме AKA, основанная на использовании XOR в ключе повторной синхронизации *AUTS* | |
| 8. | Определение активности абонента на основе полученных *SQN* | |
| 9. | Определение *MNC* и *MCC* по *SUPI* абонента | |
| 10. | Мониторинг подключающихся абонентов к сети | Рассматриваются впервые |
| 11. | DoS-атаки и DDoS-атаки на UE, используя значения *RAND, AUTN* | |
| 12. | Перехват и модификация значений *RAND, AUTN* | |
| 13. | Блокировка передачи *RAND, AUTN* | |
| 14. | Отсутствие контроля целостности значения *RAND* | |
| 15. | Передача собственных значений *RAND, AUTN* | |
| 16. | Предсказание последующих *SQN* при прямом доступе | |
| 17. | Повторное использование $RES_i$ и процедуры восстановления синхронизации после сбоя | |
| 18. | Вычисление *SUPI* методом перебора на основе полученных ответов от сети | |
| 19. | Завершение процедуры аутентификации, используя ошибку аутентификации во время проверки *SNN* | |
| 20. | Завершение процедуры аутентификации, используя ошибку аутентификации во время проверки *RES* | |

## 6. Эволюция уязвимостей процедур аутентификации сетей сотовой связи различных поколений

Эволюция уязвимостей процедур аутентификации сетей сотовой связи каждого поколения показана в таблице 6.

Таблица 6 – Уязвимости процедур аутентификации сетей сотовой связи

| № | Уязвимость | Эволюция | | | | | Публикации |
|---|---|---|---|---|---|---|---|
| | | 1G | 2G | 3G | 4G | 5G | |
| **Группа 1. Шифрование и безопасность данных** | | | | | | | |
| 1 | Отсутствуют/слабые алгоритмы шифрования | + | – | – | – | – | [33, 34, 35, 36, 37, 38, 39] |
| 2 | Возможность отключения шифрования данных через BTS | – | + | – | – | – | [42] |
| **Группа 2. Идентификаторы пользователя** | | | | | | | |
| 3 | Модификация идентификаторов пользователя | + | + | + | + | + | [41] |
| 4 | Вскрытые *SUPI* | – | – | – | + | + | [66, 67] |
| 5 | Блокировка идентификаторов пользователя | – | + | + | + | + | [64, 65] |
| 6 | Неизменность *GUTI* | – | – | – | + | – | |
| 7 | Повторное назначение *GUTI* | – | – | – | + | – | |
| 8 | Перехват идентификаторов пользователя | + | + | + | + | + | |

| № | Уязвимость | Эволюция | | | | | Публикации |
|---|---|---|---|---|---|---|---|
| | | 1G | 2G | 3G | 4G | 5G | |
| 9 | Идентификаторы пользователя передаются в открытом виде | + | + | + | + | – | [40] |
| 10 | Определение *MNC* и *MCC* по идентификатору пользователя | – | + | + | + | + | [51] |
| 11 | Проверка наличия *SUPI* в базе на основе полученных ответов от сети | – | – | – | + | + | [16] |
| 12 | Проверка наличия *IMSI* в базе на основе полученных ответов от сети | – | + | + | – | – | Рассматриваются впервые |
| 13 | Мониторинг подключающихся абонентов к сети | + | + | + | + | + | |
| 14 | Мониторинг интенсивности активности абонентов на основе запросов аутентификации | – | + | + | + | + | |
| 15 | Запрос *IMSI* без проверки подлинности | – | + | + | + | – | |
| 16 | Вычисление *SUPI* методом перебора на основе полученных ответов от сети | – | – | – | – | + | |
| **Группа 3. Синхронизация аутентификации** | | | | | | | |
| 17 | Рассинхронизация порядковых номеров аутентификации *SQN* | – | – | + | + | + | [51] |
| 18 | Определение активности абонента на основе полученных *SQN* | – | – | + | + | + | |
| 19 | Проверка наличия в базе на основе полученных ответов | – | + | + | + | + | |
| 20 | Предсказание *SQN* при прямом доступе | – | – | + | + | + | |
| **Группа 4. Безопасность ключей** | | | | | | | |
| 21 | Вскрытие индивидуального ключа пользователя $K_i$ на стороне сети | – | + | – | – | – | Рассматриваются впервые |
| 22 | Вскрытие ключа шифрования $K_C$ | – | + | – | – | – | |
| 23 | Вскрытие индивидуального ключа пользователя $K_i$ на стороне абонента | – | + | – | – | – | [42] |
| 24 | Подмена ключа шифрования | – | + | – | – | – | |
| 25 | Блокировка передачи ключа шифрования | – | + | – | – | – | |
| **Группа 5. Контроль целостности и авторства** | | | | | | | |
| 26 | Изменение содержимого запроса аутентификации от пользователя к базовой станции | + | + | + | + | + | [41] |
| 27 | Блокирование содержимого запроса аутентификации от пользователя к базовой станции | + | + | + | + | + | |
| 28 | Изменение содержимого запроса идентификации от пользователя к базовой станции | + | + | + | + | + | [40] |
| 29 | Изменение содержимого запроса идентификации от базовой станции к пользователю | – | + | + | + | – | |
| 30 | Отсутствие механизма контроля целостности сообщений при аутентификации | + | + | + | – | – | Рассматриваются впервые |
| 31 | Отсутствие механизма контроля авторства сообщений при аутентификации | + | + | + | – | – | |
| 32 | Отсутствие контроля сообщений о сбоях | + | + | + | + | + | |
| 33 | Перехват значений *RAND*, *AUTN* | – | + | + | + | + | |
| 34 | Блокировка передачи *RAND*, *AUTN* | – | + | + | + | + | |
| 35 | Передача злоумышленником собственных значений *RAND*, *AUTN* | – | + | + | + | + | |
| 36 | Повторное использование *RES* | – | + | – | – | – | |

| № | Уязвимость | Эволюция | | | | | Публикации |
|---|---|---|---|---|---|---|---|
| | | 1G | 2G | 3G | 4G | 5G | |
| 37 | Повторное использование $RES_i$ после процедуры восстановления синхронизации после сбоя | – | – | + | + | + | |
| 38 | Отсутствие контроля целостности и авторства *RES* | – | + | + | + | + | |
| 39 | Возможность закончить процедуру аутентификации, прислав раньше легитимного пользователя неправильное значение *RES* | – | + | + | + | + | |
| 40 | Повторная аутентификация в зоне, где отсутствует абонент, используя вычисленный ключ $K_i$ | – | + | – | – | – | |
| 41 | Завершение процедуры аутентификации, используя модификацию запросов неправильными значениями | – | + | + | + | + | |
| 42 | Завершение процедуры аутентификации, используя ошибку аутентификации во время проверки *SNN* | – | – | – | – | + | |
| 43 | Определение наличия абонента по полученному ответу обработки ошибки | – | – | + | + | + | [51] |
| 44 | Уязвимость в механизме AKA, основанная на использовании XOR в ключе повторной синхронизации *AUTS* | – | – | + | + | + | |
| 45 | Атака на конфиденциальность местоположения | – | – | – | – | + | |
| **Группа 6. Базовая станция и устройство пользователя** | | | | | | | |
| 46 | Отсутствует аутентификация базовой станции | + | + | – | – | – | [42] |
| 47 | Возможность проведения DoS-атаки на UE и элементы сети | + | + | + | + | + | [51] |
| 48 | Подключение IMSI-перехватчика | + | + | + | + | + | |
| 49 | Атака на конфиденциальность местоположения абонента | – | – | – | – | + | [16] |
| 50 | Возможность осуществления DoS- и DDoS-атак, используя запрос к сети и запрос к устройству абонента во время инициализации | – | + | – | – | – | [40] |
| 51 | Осуществление DoS- и DDoS-атак легитимными устройствами абонентов сети, используя запрос идентификации от базовой станции | – | + | – | – | – | Рассматриваются впервые |
| 52 | Переполнение буфера в оборудовании сети во время процедуры аутентификации | + | + | + | + | + | |
| 53 | Переполнение буфера в устройстве абонента во время процедуры аутентификации | + | + | + | + | + | |
| 54 | Разрыв процедуры аутентификации, вызванный созданными задержками в передаче информации | – | + | + | + | + | |

Сравнительный анализ процедур аутентификации сетей сотовой связи различных поколений показывает, что ряд уязвимостей этих процедур остаются актуальными, несмотря на многочисленные улучшения и внедрение новых методов защиты. Здесь следует отметить три основных момента.

1. В сетях 2G и 3G идентификатор пользователя *IMSI* передавался в незашифрованном виде, что создавало предпосылку для перехвата. В сетях 4G и 5G для устранения этой уязвимости введены временные идентификаторы *GUTI*, *SUPI* и *SUCI*. Однако возможность их перехвата и расшифровки по-прежнему сохраняется. Это позволяет злоумышленнику отслеживать местоположение пользователей и проводить множество атак (в т.ч. пейджинга и зондирования).

2. Уязвимости в протоколе управления радиоресурсами RRC позволяют злоумышленникам разрывать соединения и проводить DoS-атаки на UE и элементы сети. На текущий момент проведение DoS-атак остается актуальным во всех поколениях сотовой связи.

3. Уязвимость механизма использования сообщений о сбоях также остается актуальной проблемой для конфиденциальности пользователей.

## 7. Закономерности в характере происхождения уязвимостей процедур аутентификации сетей сотовой связи различных поколений

Результаты анализа процедур аутентификации сетей сотовой связи от первого до пятого поколений позволили выявить следующие ключевые закономерности в характере происхождения их уязвимостей.

Первая закономерность состоит в том, что в сетях сотовой связи существуют уязвимости, которые устранить в принципе невозможно. Ведь сеть сотовой связи изначально предполагает возможность неподконтрольного подключения к ней любого устройства по радиоканалу. Для того, чтобы подключиться к сети и работать с ней с использованием самых криптостойких алгоритмов шифрования, это устройство должно без шифрования начать общаться с сетью. А значит можно найти возможность для радиоперехвата и последующей атаки типа «человек посередине».

Вторая закономерность состоит в том, что разработчики очередного поколения стандарта сотовой связи шли по пути устранения уязвимостей, обнаруженных в ходе эксплуатации сетей предыдущего поколения. То есть имеет место классическая для крупных забюрократизированных систем, к которым в том числе относится консорциум 3GPP, рефлексивная концепция, когда решается очевидная проблема, а гипотетическая проблема не является очевидной и «авось не являться таковой». Ведь на «доходчивое» доказательство и последующее разрешение гипотетической проблемы всегда требуются дополнительные ресурсы, которые в крупной системе обычно весьма ограничены. Здесь уместна аналогия с постановкой светофоров в тех местах, где уже неоднократно случались аварии с тяжкими последствиями. Возможно ли искоренить это?

В рамках рефлексивной концепции разработчики стандартов в 3GPP, очевидно, опирались преимущественно на эмпирический (предположение и последующая проверка) и феноменологический (накопление фактов и их осмысление) методы поиска уязвимостей. Эти методы, как показано в [43], не позволяют не то, что выявить полное множество уязвимостей, но даже сколь угодно системно подойти к решению этой задачи.

Частичное применение в настоящем исследовании изложенного в [43] метода генерации кибератак на телекоммуникационное оборудование, позволяющего синтезировать необходимое и достаточное множество тестовых способов реализации кибератак на телекоммуникационное оборудование, дало возможность выявить значительное количество потенциальных уязвимостей сетей сотовой связи, которые существовали еще в сетях сотовой связи 2G и из-за своей «неопубликованности» во многом сохранились в сетях 5G.

## Направления дальнейших исследований

Безусловно, каждую из выявленных потенциальных уязвимостей необходимо проверить на практике, что является первым направлением развития результатов настоящего исследования – практическим направлением. По сути, в этом и состоит полноценное применение вышеуказанного метода генерации кибератак на телекоммуникационное оборудование, с использованием которого новые потенциальные уязвимости и были найдены. Неискушенный читатель может усомниться в необходимости такой работы. Однако, как показывает практика, даже если хотя бы одна из найденных потенциальных уязвимостей является реальной, то это уже создает проблему безопасности сети. А, как известно, реальность потенциальной уязвимости во многом определяется искусностью разработчиков соответствующих средств реализации компьютерных атак. И то, что сегодня может не удастся одному разработчику, в будущем (или неопубликованном настоящем) может оказаться «по зубам» другому разработчику. Ведь цена таких уязвимостей сегодня весьма высока.

Вторым направлением развития результатов настоящего исследования – теоретическим направлением – является моделирование работы сетей сотовой связи в условиях компьютерных атак, эксплуатирующих рассмотренные уязвимости, в интересах установления допустимых параметров функционирования этих сетей для учета их в соответствующих механизмах защиты и разработки дополнительных мер по минимизации потенциальных рисков.

## Заключение

Таким образом, в настоящей работе приведено описание процедур аутентификации сетей сотовой связи с первого по пятое поколения, показаны опубликованные уязвимости этих процедур, а также с использованием метода генерации кибератак на телекоммуникационное оборудование сформированы предложения по эксплуатации новых, ранее не исследованных потенциальных уязвимостей. Системный анализ эволюции уязвимостей сетей сотовой связи пяти стандартизованных поколений позволил выявить ключевые закономерности в характере их происхождения. Во-первых, в сетях сотовой связи существуют уязвимости, которые устранить в принципе невозможно. А, во-вторых, разработчики очередного поколения стандарта сотовой связи шли по пути устранения уязвимостей, обнаруженных в ходе эксплуатации сетей предыдущего поколения, и не уделяли внимания системному рассмотрению соответствующих процедур в интересах выявления наиболее полного множества уязвимостей. Для разработки эффективных способов противодействия средствам реализации компьютерных атак, эксплуатирующим новые потенциально возможные уязвимости, требуется проведение исследований, направленных на проверку на практике каждой из выявленных потенциальных уязвимостей и моделирование работы сетей сотовой связи в условиях компьютерных атак, эксплуатирующих выявленные потенциальные уязвимости. Эти результаты свидетельствуют о необходимости совершенствования процедур аутентификации в сетях сотовой связи с учетом рассмотренных уязвимостей в интересах повышения эффективности противодействия средствам их реализации.

## Литература

1. Taylor P. Number of Mobile GSM/EDGE Subscriptions Worldwide by Region from 2011 to 2028 // Statista [Электронный ресурс]. 10.05.2024 – URL: https://www.statista.com/statistics/521606/wcdma-hspa-mobile-subscriptions-worldwide/ (дата обращения: 28.09.2024).

2. Taylor P. Number of LTE Subscriptions Worldwide from 2011 to 2028, by region // Statista [Электронный ресурс]. 18.07.2023 – URL: https://www.statista.com/statistics/1016008/volte-subscriptions-worldwide-by-region/ (дата обращения: 28.09.2024).

3. Taylor P. Number of LTE Subscriptions Worldwide from 2018 to 2023 (in billions) // Statista [Электронный ресурс]. 18.01.2023 – URL: https://www.statista.com/statistics/206615/forecast-of-the-number-of-global-hspa-lte-subscriptions-up-to-2014/ (дата обращения: 28.09.2024).

4. Жабин А. На создание сети 5G в регионах может быть выделено только 27 млрд руб. из госбюджета // Коммерсантъ [Электронный ресурс]. 13.09.2024 – URL: https://www.kommersant.ru/doc/7084299 (дата обращения: 28.09.2024).

5. Cisco Annual Internet Report (2018–2023) // Cisco Public [Электронный ресурс]. 2023 – URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf (дата обращения: 23.09.2024).

6. Scahill J., Greenwald G. The NSA's Secret Role in the U.S. Assassination Program // The Intercept [Электронный ресурс]. 10.02.2014. – URL: https://theintercept.com/2014/02/10/the-nsas-secret-role/ (дата обращения: 23.09.2024).

7. Porter T. Israel Reportedly Planted Tiny Surveillance Devices Near the White House to Spy on Donald Trump, but Faced no Consequences // Business Insider [Электронный ресурс]. 12.09.2019. – URL: https://www.businessinsider.com/israel-planted-devices-near-white-house-spy-on-trump-report-2019-9 (дата обращения: 23.09.2024).

8. Храмцов И. А. Основные уязвимости сетей поколения GSM // Форум молодых ученых. 2019. № 2. С. 1584–1587.

9. Khan M., Ahmed A., Cheema A. Vulnerabilities of UMTS Access Domain Security Architecture // Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. 2008. С. 350–355. doi: 10.1109/SNPD.2008.78.

10. Donda D. IMEI Tracker – Track Phone Using IMEI Online Free // iStaunch [Электронный ресурс]. 09.02.2024. – URL: https://www.istaunch.com/imei-tracker/ (дата обращения: 23.09.2024).

11. Kareem K. The Impact of IMSI Catcher Deployments on Cellular Network Security: Challenges and Countermeasures in 4G and 5G Networks // International Journal on Recent and Innovation Trends in Computing and Communication. 2024. С. 3871–3879, doi: 10.7910/DVN/6JPQWO.

12. Broek F. V., Verdult R., Ruiter J. D. Defeating IMSI Catchers // Proceedings of the 22nd ACM SIGSAC Conference on Computer and

Communications Security (Нью Йорк, 12 октября 2015 г.). – Нью Йорк, 2015. – С. 340–351.

13. Яковлев В. С. Процедура проверки подлинности в GSM // Достижения вузовской науки. 2016. № 20. С. 183–187.

14. Мазуркевич Д. О. Особенности архитектуры систем безопасности в сетях сотовой связи разных поколений // Фундаментальные проблемы радиоэлектронного приборостроения. 2009. № 4. С. 229–233.

15. Данилин М. И. Обзор угроз безопасности стандарта LTE // Форум молодых ученых. 2021. № 6(58). С. 264–268.

16. Бельский В. С., Дрынкин А. В., Давыдов С. А. Вопросы обеспечения безопасности абонентов в сетях радиодоступа пятого поколения // International Journal of Open Information Technologies. 2021. № 7. С. 32–55.

17. Bisht K., Chimnani P., Marwal R. Mobile Phone Cloning // Iconic Research and Engineering Journals, 2018. 5 с.

18. Mobile identification number // Википедия: свободная энциклопедия [Электронный ресурс]. – URL: https://en.wikipedia.org/wiki/Mobile_identification_number (дата обращения: 23.09.2024).

19. Hanser C., Moritz S., Zaloshnja F. Security in Mobile Telephony: The Security Levels in the Different Handy Generations // Computer Science, Engineering, 2005. 14 с.

20. ETSI TS 123 002 V14.1.0 “Digital Cellular Telecommunications System (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Circuit Switched (CS) Fallback in Evolved Packet System (EPS); Stage 2” // ETSI [Электронный ресурс]. – URL: https://www.etsi.org/deliver/etsi_ts/123200_123299/123272/14.01.00_60/ts_123272v140100p.pdf (дата обращения: 23.09.2024).

21. ETSI TS 151 011 V4.15.0 “Digital Cellular Telecommunications System (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface” // ETSI [Электронный ресурс]. – URL: https://www.etsi.org/deliver/etsi_TS/151000_151099/151011/04.05.00_60/ts_151011v040500p.pdf (дата обращения: 23.09.2024).

22. 3GPP TS 11.11 V8.14.0 (2007-06) “3rd Generation Partnership Project; Technical Specification Group Terminals Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface (Release 1999)” // 3GPP [Электронный ресурс]. – URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=419 (дата обращения: 28.11.2024).

23. 3GPP TS 43.020 “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Related Network Functions (Release 4)” // 3GPP [Электронный ресурс]. – URL: https://www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/Old_Vsns/43020-400.pdf (дата обращения: 23.09.2024).

24. 3GPP TS 23.003 V19.0.0 (2024-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network and

Terminals; Numbering, Addressing and Identification; (Release 19) // ARIB [Электронный ресурс]. – URL: https://www.arib.or.jp/english/html/overview/doc/STD-T63v10_20/5_Appendix/Rel8/23/23003-8i0.pdf (дата обращения: 23.09.2024).

25. A5/1 Decryption // OpenSource [Электронный ресурс]. 2010. – URL: https://opensource.srlabs.de/projects/a51-decrypt/files (дата обращения: 23.09.2024).

26. Kalenderi M., Pnevmatikatos D. N., Papaefstathiou I., Manifavas C. Breaking the GSM A5/1 Cryptography Algorithm with Rainbow Tables and High-End FPGAS // 22nd International Conference on Field Programmable Logic and Applications. 2012. С. 747–753.

27. 3GPP TSG-SA WG3 (Security) “SP-070671 – Prohibiting A5/2 in mobile stations and other clarifications regarding A5 algorithm support“ // 3GPP [Электронный ресурс]. – URL:http://portal.3gpp.org/ngppapp/DownloadTDoc.aspx?contributionUid=SP-070593 (дата обращения: 28.11.2024).

28. Biham E., Dunkelman O., Keller N. A Related-Key Rectangle Attack on the Full KASUMI // Advances in Cryptology – ASIACRYPT. 2005. С. 443–461.

29. Kuhn U. Cryptanalysis of Reduced-round MISTY // Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology. 2001. doi: 10.1007/3-540-44987-6-20.

30. Dunkelman O., Keller N., Shamir A. A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony // International Association for Cryptologic Research Eprint. 2010. 13 с.

31. Бойко А. А., Гриценко С. А. Модель применения авиационного модуля нарушения доступности абонентских терминалов сотовой связи для круговой траектории полета // Вестник Воронежского государственного университета. 2013. № 2. С. 58–65.

32. Dabrowski A., Pianta N., Klepp T. IMSI-catch me if you can: IMSI-catcher-catchers // Proceedings of the Annual Computer Security Applications Conference. 2014. doi: 10.1145/2664243.2664272.

33. Josang A., Miralabé L., Dallot L. Vulnerability by Design in Mobile Network Security // Journal of Information Warfare. 2015. С. 86–98.

34. Golic J. D. Cryptanalysis of Alleged A5 Stream Cipher // Volume 1233 of Lec-ture Notes in Computer Science. 1997. С. 239–255.

35. Biryukov A., Shamir A., Wagner D. Real-time Cryptanalysis of A5/1 on a PC // Lecture Notes in Computer Science. 1978. С. 1–18.

36. Barkan E., Biham E., Keller N. Instant Ciphertext-only Cryptanalysis of GSM Encrypted Communication // Journal of Cryptology. 2003. С. 392–429.

37. Ekdahl P., Johansson T. Another Attack on A5/1 // IEEE Transactions on Information Theory. 2008. С. 284–289.

38. Maximov A., Johansson T., Babbage S. An Improved Correlation Attack on A5/1 // Lecture Notes in Computer Science. 2004. С. 1–18.

39. 27c3: Wideband GSM Sniffing // 27th Chaos Communication Congress 27c3: Wideband GSM Sniffing // RuTube [Электронный ресурс]. – URL:

https://rutube.ru/video/48e5ae8a536a28a261de0e4531a2e612/ (дата обращения: 04.10.2024).

40. Bocan V., Cretu V. Mitigating Denial of Service Threats in GSM Networks // Availability, Reliability and Security. 2006. 6 с.

41. Перегудов М. А., Уманский А. Я., Жданова А. А., Храмов В. Ю. Распределенная система противодействия несанкционированному доступу к информации абонентов сотовой связи // Системы управления, связи и безопасности. 2022. № 2. С. 149–172. doi 10.24412/2410-9916-2022-2-149-172.

42. Wray S. COMP128: A Birthday Surprise // Stuart Wray [Электронный ресурс]. – URL: http://www.stuartwray.net/comp128-a-birthday-surprise-rev.pdf (дата обращения: 02.11.2024).

43. Бойко А. А. Киберзащита автоматизированных систем воинских формирований. – СПб.: Наукоемкие технологии, 2021. – 300 с.

44. Farhoomand A. F., Mak V. NTT DoCoMo: Establishing Global 3G Standards // University of Hong Kong. 2003. 33 с.

45. Ulhaq I., Shafiq A., Yahya K., Iqbal N. Cell Breathing and Cell Capacity in CDMA: Algorithm & evaluation. // 7th International Symposium on Communication Systems, Networks and Digital Signal Processing. 2010. С. 432–436.

46. ETSI TS 133 102 V11.5.1 “Digital Cellular Telecommunications System (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); 3G Security; Security Architecture (3GPP TS 33.102 version 15.0.0 Release 15)” // ETSI [Электронный ресурс]. – URL: https://www.etsi.org/deliver/etsi_ts/133100_133199/133102/15.00.00_60/ts_133102v150000p.pdf (дата обращения: 23.09.2024).

47. ETSI TS 123 012 V8.2.0 (2009-09) Technical Specification Digital cellular Telecommunications System (Phase 2+); Universal Mobile Telecommunications System (UMTS); Location Management Procedures (3GPP TS 23.012 version 8.2.0 Release 8) // ETSI [Электронный ресурс]. – URL: https://www.etsi.org/deliver/etsi_ts/123000_123099/123012/08.02.00_60/ts_123012v080200p.pdf (дата обращения: 23.09.2024).

48. Tsay J., Mjølsnes S. F. A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols // Mathematical Methods, Models, and Architectures for Network Security Systems. 2012.

49. Meyer U., Wetzel S. On the Impact of GSM Encryption and Man-in-the-middle Attacks on the Security of Interoperating GSM/UMTS Networks // Personal, Indoor and Mobile Radio Communications. 2004. С. 2876–2883.

50. Invasive Phone Tracking: New SS7 Research Blows the Lid off Personal Security // ZDNET [Электронный ресурс]. 2014. – URL: https://www.zdnet.com/article/invasive-phone-tracking-new-ss7-research-blows-the-lid-off-personal-security/ (дата обращения: 23.09.2024).

51. Borgaonkar R., Hirschi L., Park S., Shaik A. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols // PoPETs. 2019. С. 108–127.

52. Introduction to Mobile Networks – 3G – STEEMIT [Электронный ресурс]. – URL: https://steemit.com/mobilenetworks/@irelandscape/introduction-to-mobile-networks-3g-umts-authentication (дата обращения: 04.10.2024).

53. IMSI-catchers // PKI Electronic [Электронный ресурс]. 01.07.2016. – URL: https://pki-electronic.com/products/imsi-catcher/imsi-catcher/ (дата обращения: 23.09.2024).

54. The Big Black Book of Electronic Surveillance: 5th edition (3BES5) // Youtube [Электронный ресурс]. 01.07.2016. – URL: https://c5is.com/wp-content/uploads/2016/12/3BES-5th-Edition-2017-FINAL.pdf (дата обращения: 23.09.2024).

55. 4G. LTE – Long Term Evolution [Электронный ресурс]. – URL: https://celnet.ru/4G.php (дата обращения: 04.10.2024).

56. LTE (Telecommunication) // Википедия: свободная энциклопедия [Электронный ресурс]. – URL: https://en.wikipedia.org/wiki/LTE_(telecommunication) (дата обращения: 04.10.2024).

57. Эволюция LTE и NR // Хабр [Электронный ресурс]. – URL: https://habr.com/ru/articles/723426/ (дата обращения: 04.10.2024).

58. 3GPP TS 23.401 V13.6.1 (2016-03) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 13) // ARIB [Электронный ресурс]. – URL: https://www.arib.or.jp/english/html/overview/doc/STD-T63V12_00/5_Appendix/Rel13/23/23401-d61.pdf (дата обращения: 23.09.2024).

59. Farivar C. Cities Scramble to Upgrade “Stingray Tracking as End of 2G Network Looms" // Ars Technica [Электронный ресурс]. 10.05.2024 – URL: https://arstechnica.com/tech-policy/2014/09/cities-scramble-to-upgrade-stingray-tracking-as-end-of-2g-network-looms/ (дата обращения: 23.09.2024).

60. Martone Radio Technology, "MRT – Products [Электронный ресурс]. – URL: http://zblgeo.com/content/products/ (дата обращения: 23.09.2024).

61. Новые уязвимости 4G LTE: массовая рассылка сообщений, имперсонификация абонентских устройств и другие // Habr [Электронный ресурс]. 19.03.2018 – URL: https://habr.com/ru/companies/globalsign/articles/351470/ (дата обращения: 02.11.2024).

62. 3GPP TR 33.899 V1.3.0 (2017-08) Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14) // 3GPP [Электронный ресурс]. – URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045 (дата обращения: 17.11.2024).

63. 3GPP TS 33.501 V19.0.0 (2024-09) Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 19) // 3GPP [Электронный ресурс]. – URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169 (дата обращения: 17.11.2024).

64. Arapinis M., Mancini L., Ritter E., Ryan M. Analysis of Privacy in Mobile Telephony Systems // International Journal of Information Security. 2017. С. 491–523.

65. Shaik A, Seifert J., Borgaonkar R., Asokan N., Niemi V. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems // 23rd Annual Network and Distributed System Security Symposium. – Сан Диего, 2016.

66. Khan H, Dowling B., Martin K. Identity Confidentiality in 5G Mobile Telephony Systems // 4th International Conference SSR. Дармштадт, 2018.

67. Shor P. Algorithms for quantum computation: Discrete logarithms and factoring // 35th Annual Symposium on Foundations of Computer Science. 1994. С. 124–134.

68. 3GPP TS 23.501 V15.4.0 (2018-12) Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 15) // 3GPP [Электронный ресурс]. – URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144 (дата обращения: 17.11.2024).

69. Khan H., Martin K. On the Efficacy of New Privacy Attacks Against 5G AKA // 16th International Joint Conference on e-Business and Telecommunications. 2019. С. 431–438.

**References**

1. Taylor P. Number of Mobile GSM/EDGE Subscriptions Worldwide by Region from 2011 to 2028. *Statista*, 10 May 2024. Available at: https://www.statista.com/statistics/521606/wcdma-hspa-mobile-subscriptions-worldwide/ (accessed 23 September 2024).

2. Taylor P. Number of LTE Subscriptions Worldwide from 2011 to 2028, by Region. *Statista*, 18 July 2023. Available at: https://www.statista.com/statistics/1016008/volte-subscriptions-worldwide-by-region/ (accessed 23 September 2024).

3. Taylor P. Number of LTE Subscriptions Worldwide from 2018 to 2023 (in billions). *Statista*, 18 January 2023. Available at: https://www.statista.com/statistics/206615/forecast-of-the-number-of-global-hspa-lte-subscriptions-up-to-2014/ (accessed 23 September 2024).

4. Zhabin A. Na sozdanie seti 5G v regionah mozhet byt' vydeleno tol'ko 27 mlrd rub. iz gosbyudzheta [Only 27 Billion Rubles from the State Budget Can be Allocated for the Creation of a 5G Network in the Regions]. *Kommersant*, 13 September 2024. Available at: https://www.kommersant.ru/doc/7084299 (accessed 23 September 2024) (in Russian).

5. Cisco Annual Internet Report (2018–2023) White Paper. 2023. Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf (accessed 23 September 2024).

6. The NSA’s Secret Role in the U.S. Assassination Program. *The Intercept*, 10 February 2014. Available at: https://theintercept.com/2014/02/10/the-nsas-secret-role/ (accessed 23 September 2024).

7. Israel Reportedly Planted Tiny Surveillance Devices near the White House to Spy on Donald Trump, but Faced no Consequences. *Business Insider*, 12

September 2019. Available at: https://www.businessinsider.com/israel-planted-devices-near-white-house-spy-on-trump-report-2019-9 (accessed 23 September 2024).

8. Hramcov I. A. Osnovnye uyazvimosti setej pokoleniya GSM [The Main Vulnerabilities of GSM Generation Networks]. *Forum molodyh uchenyh* [Forum of Young Scientists], 2019, no. 2, pp. 1584–1587 (in Russian).

9. Khan M., Ahmed A., Cheema A. Vulnerabilities of UMTS Access Domain Security Architecture. *Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2008, pp. 350–355. doi: 10.1109/SNPD.2008.78.

10. Donda D. IMEI Tracker – Track Phone Using IMEI Online Free. *iStaunch*, 09 February 2024. Available at: https://www.istaunch.com/imei-tracker/ (accessed 23 September 2024).

11. Kareem K. The Impact of IMSI Catcher Deployments on Cellular Network Security: Challenges and Countermeasures in 4G and 5G Networks. *International Journal on Recent and Innovation Trends in Computing and Communication*, 2024, pp. 3871–3879. doi: 10.7910/DVN/6JPQWO.

12. Broek F. V., Verdult R., Ruiter J. D. Defeating IMSI Catchers. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security – New-York, 2015, pp. 340–351.

13. Yakovlev V. S. Procedura proverki podlinnosti v GSM [GSM Authentication Procedure] *Dostizheniya vuzovskoj nauki* [Achievements of University Science] 2016, no. 20, pp. 183–187 (in Russian).

14. Mazurkevich D. O. Osobennosti arhitektury sistem bezopasnosti v setyah sotovoj svyazi raznyh pokolenij [Features of the Architecture of Security Systems in Cellular Networks of Different Generations] *Fundamental'nye problemy radio-elektronnogo priborostroeniya*. [Fundamental Problems of Radio-electronic Instrumentation], 2009, no. 4, pp. 229–233 (in Russian).

15. Danilin M. I. Obzor ugroz bezopasnosti standarta LTE [Overview of LTE Security Threats] *Forum molodyh uchenyh*. [Forum of Young Scientists], 2021, no. 6(58), pp. 264–268 (in Russian).

16. Bel'skij V. S., Drynkin A. V., Davydov S. A. Voprosy obespecheniya bezopasnosti abonentov v setyah radiodostupa pyatogo pokoleniya [Issues of Ensuring Subscriber Security in Fifth-generation Radio Access Networks] *International Journal of Open Information Technologies*, 2021, no. 7, pp. 32–55 (in Russian).

17. Bisht K., Chimnani P., Marwal R. Mobile Phone Cloning. *Iconic Research and Engineering Journals*, 2018. 5 p.

18. Mobile Identification Number. Wikipedia. Available at: https://en.wikipedia.org/wiki/Mobile_identification_number (accessed 23 September 2024).

19. Hanser C., Moritz S., Zaloshnja F. Security in Mobile Telephony: The Security Levels in the Different Handy Generations, Uppsala Universitet, Uppsala, 2005. 2 p.

20. ETSI TS 123 002 V14.1.0. Digital Cellular Telecommunications System (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Circuit Switched (CS) Fallback in Evolved Packet System (EPS); Stage 2, European Telecommunications Standards Institute, 2007. 107 p. Available at: https://www.etsi.org/deliver/etsi_ts/123200_123299/123272/14.01.00_60/ts_123272v140100p.pdf (accessed 23 September 2024).

21. ETSI TS 151 011 V4.15.0. Digital Cellular Telecommunications System (Phase 2+); Specification of the Subscriber Identity Module. Mobile Equipment (SIM-ME) Interface, European Telecommunications Standards Institute, 2002. 173 p. Available at: https://www.etsi.org/deliver/etsi_TS/151000_151099/151011/04.05.00_60/ts_151011v040500p.pdf (accessed 23 September 2024).

22. 3GPP TS 11.11 V8.14.0 (2007-06) "3rd Generation Partnership Project; Technical Specification Group Terminals Specification of the Subscriber Identity Module – Mobile Equipment (SIM - ME) interface (Release 1999)". 3rd Generation Partnership Project. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=419 (accessed 28 November 2024).

23. 3GPP TS 43.020 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Related Network Functions (Release 4). 3rd Generation Partnership Project. Available at: https://www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/Old_Vsns/43020-400.pdf (accessed 23 September 2024).

24. 3GPP TS 23.003 V19.0.0 (2024-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, Addressing and Identification; (Release 19) ARIB. Available at: https://www.arib.or.jp/english/html/overview/doc/STD-T63v10_20/5_Appendix/Rel8/23/23003-8i0.pdf (accessed 23 September 2024).

25. A5/1. Wikipedia Russia. Available at: https://opensource.srlabs.de/projects/a51-decrypt/files (accessed 23 September 2024).

26. Kalenderi M., Pnevmatikatos D. N., Papaefstathiou I., Manifavas C. Breaking the GSM A5/1 Cryptography Algorithm with Rainbow Tables and High-end FPGAS. 22nd International Conference on Field Programmable Logic and Applications, 2012. pp. 747–753.

27. 3GPP TSG-SA WG3 (Security) "SP-070671 – Prohibiting A5/2 in mobile stations and other clarifications regarding A5 algorithm support". 3rd Generation Partnership Project. Available at: http://portal.3gpp.org/ngppapp/DownloadTDoc.aspx?contributionUid=SP-070593 (accessed 28 November 2024).

28. Biham E., Dunkelman O., Keller N. A Related-Key Rectangle Attack on the Full KASUMI. *Advances in Cryptology*. ASIACRYPT, 2005. pp. 443–461.

29. Kuhn U. Cryptanalysis of Reduced-round MISTY. *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*. 2001. doi: 10.1007/3-540-44987-6-20.

30. Dunkelman O., Keller N., Shamir A. A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony. *International Association for Cryptologic Research*. 2010. 13 p.

31. Boiko A. A., Gritsenko S. A. Model of Application of Aviation Module Violation of Availability of Subscriber Cellular Terminals for Circular Flight Path. *Bulletin of Voronezh state technical University*, 2013, no. 2, pp. 58–65 (in Russian).

32. Dabrowski A, Pianta N., Klepp T. IMSI-catch me if you can: IMSI-catcher-catchers. *Proceedings of the Annual Computer Security Applications Conference*, 2014. doi: 10.1145/2664243.2664272.

33. Josang A., Miralabé L., Dallot L. Vulnerability by Design in Mobile Network Security. *Journal of Information Warfare*, 2015, pp. 86–98.

34. Golic J. D. Cryptanalysis of Alleged A5 Stream Cipher. *Lecture Notes in Computer Science*, 1997, vol. 1233, pp. 239–255.

35. Biryukov A., Shamir A., Wagner D. Real-time Cryptanalysis of A5/1 on a PC. *Lecture Notes in Computer Science*, 2002, pp. 1–18.

36. Barkan E., Biham E., Keller N. Instant Ciphertext-only Cryptanalysis of GSM Encrypted Communication. *Journal of Cryptology*, 2003, pp. 392–429.

37. Ekdahl P., Johansson T. Another Attack on A5/1. *IEEE Transactions on Information Theory*, 2008, pp. 284–289.

38. Maximov A., Johansson T., Babbage S. An Improved Correlation Attack on A5/1. *Lecture Notes in Computer Science*, 2004, pp. 1–18.

39. 27th Chaos Communication Congress 27c3: Wideband GSM Sniffing. RuTube. 04.10.2024. Available at: https://rutube.ru/video/48e5ae8a536a28a261de0e4531a2e612/ (accessed 23 September 2024).

40. Bocan V., Cretu V. Mitigating Denial of Service Threats in GSM Networks. *Availability, Reliability and Security*. 2006. 6 p.

41. Peregudov M. A., Umanskiy A. Ya., Zhdanova A. A., Khramov V. Yu. Distributed System to Counter Unauthorized Access to Cellular Subscribers Information. *Systems of Control, Communication and Security*, 2022, no. 2, pp. 149-172. doi: 10.24412/2410-9916-2022-2-149-172 (in Russian).

42. Wray S. COMP128: A Birthday Surprise. Available at: http://www.stuartwray.net/comp128-a-birthday-surprise-rev.pdf (accessed 02 November 2024).

43. Boiko A. A. *Kiberzashchita avtomatizirovannykh sistem voinskikh formirovanii* [Cyberprotection of Automated Systems of Military Formations]. Saint Petersburg, Naukoemkie tekhnologii Publ., 2021. 300 p. (in Russian).

44. Farhoomand A. F., Mak V. NTT DoCoMo: Establishing Global 3G Standards. University of Hong Kong, 2003. 33 p.

45. Ulhaq I., Shafiq A., Yahya K., Iqbal N. Cell Breathing and Cell Capacity in CDMA: Algorithm & evaluation. *7th International Symposium on Communication Systems, Networks and Digital Signal Processing*, 2010, pp. 432–436.

46. ETSI TS 133 102 V11.5.1. Digital Cellular Telecommunications System (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); 3G security; Security Architecture (3GPP TS 33.102 version 15.0.0 Release 15)

European Telecommunications Standards Institute, 2018. 79 p. Available at: https://www.etsi.org/deliver/etsi_ts/133100_133199/133102/15.00.00_60/ts_133102v150000p.pdf (accessed 23 September 2024).

47. ETSI TS 123 012 V8.2.0 (2009-09) Technical Specification Digital Cellular Telecommunications System (Phase 2+); Universal Mobile Telecommunications System (UMTS); Location Management Procedures (3GPP TS 23.012 version 8.2.0 Release 8) 2018. 79 p. Available at: https://www.etsi.org/deliver/etsi_ts/133100_133199/133102/15.00.00_60/ts_133102v150000p.pdf (accessed 23 September 2024).

48. Tsay J., Mjølsnes S. F. A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols. *Mathematical Methods, Models, and Architectures for Network Security Systems*, 2012.

49. Meyer U., Wetzel S. On the Impact of GSM Encryption and Man-in-the-middle Attacks on the Security of Interoperating GSM/UMTS Networks. *Personal, Indoor and Mobile Radio Communications*, 2004, pp. 2876–2883.

50. Invasive Phone Tracking: New SS7 Research Blows the Lid off Personal Security. *ZDNET*, 2014. Available at: https://www.zdnet.com/article/invasive-phone-tracking-new-ss7-research-blows-the-lid-off-personal-security/ (accessed 23 September 2024).

51. Borgaonkar R., Hirschi L., Park S., Shaik A. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. *PoPETs*, 2019, pp. 108–127.

52. Introduction to Mobile Networks – 3G. *STEEMIT* Available at: https://steemit.com/mobilenetworks/@irelandscape/introduction-to-mobile-networks-3g-umts-authentication (accessed 23 September 2024).

53. IMSI-catchers. PKI electronic. 01.07.2016. Available at: https://pki-electronic.com/products/imsi-catcher/imsi-catcher/ (accessed 23 September 2024).

54. The Big Black Book of Electronic Surveillance: 5th edition (3BES5) Youtube, 23.09.2024. Available at: https://c5is.com/wp-content/uploads/2016/12/3BES-5th-Edition-2017-FINAL.pdf (accessed 23 September 2024).

55. 4G. LTE – Long Term Evolution. Celnet. Available at: https://celnet.ru/4G.php (accessed 23 September 2024) (in Russian).

56. LTE (Telecommunication). Wikipedia. Available at: https://en.wikipedia.org/wiki/LTE_(telecommunication) (accessed 23 September 2024).

57. Evolyuciya LTE i NR [Evolution of LTE and NR] Habr. Available at: https://habr.com/ru/articles/723426/ (accessed 23 September 2024) (in Russian).

58. 3GPP TS 23.401 V13.6.1 (2016-03) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 13). ARIB. Available: https://www.arib.or.jp/english/html/overview/doc/STD-T63V12_00/5_Appendix/Rel13/23/23401-d61.pdf (accessed 23 September 2024).

59. Farivar C. Cities Scramble to Upgrade “Stingray” Tracking as End of 2G Network Looms. Ars Technica, 1 September 2014. Available at:

https://arstechnica.com/tech-policy/2014/09/cities-scramble-to-upgrade-stingray-tracking-as-end-of-2g-network-looms/ (accessed 23 September 2024).

60. Martone Radio Technology, MRT–Products. Available: http://zblgeo.com/content/products (accessed 23 September 2024).

61. Novye uyazvimosti 4G LTE: massovaya rassylka soobshchenij, impersonifikaciya abonentskih ustrojstv i drugie [New 4G LTE Vulnerabilities: Mass Messaging, Impersonation of Subscriber Devices and Others]. Habr. Available at: https://habr.com/ru/companies/globalsign/articles/351470/ (accessed 02 November 2024) (in Russian).

62. 3GPP TR 33.899 V1.3.0 (2017-08) Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14). 3rd Generation Partnership Project, 2017. 605 p. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045 (accessed 17 November 2024).

63. 3GPP TS 33.501 V19.0.0 (2024-09) Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 19). 3rd Generation Partnership Project, 2024. 333 p. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169(accessed 17 November 2024).

64. Arapinis M., Mancini L., Ritter E., Ryan M. Analysis of Privacy in Mobile Telephony Systems. *International Journal of Information Security*, 2017, pp. 491–523.

65. Shaik A, Seifert J., Borgaonkar R., Asokan N., Niemi V. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. *23rd Annual Network and Distributed System Security Symposium*, San Diego, February 2016.

66. Khan H, Dowling B., Martin K. Identity Confidentiality in 5G Mobile Telephony Systems. *4th International Conference SSR 2018*, 2018, pp. 120–142.

67. Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

68. 3GPP TS 23.501 V15.4.0 (2018-12) Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 15). 3rd Generation Partnership Project, 2018. 236 p. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144 (accessed 17 November 2024).

69. Khan H., Martin K. On the Efficacy of New Privacy Attacks Against 5G AKA. *16th International Joint Conference on e-Business and Telecommunications*, 2019, pp. 431–438.

**Статья поступила 19 ноября 2024 г.**

## Информация об авторах

*Бойко Алексей Александрович* – доктор технических наук, доцент. Преподаватель. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: методы и системы защиты информации, методы оценки эффективности сложных систем. E–mail: albo@list.ru

*Быков Михаил Юрьевич* – адъюнкт. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: информационная безопасность систем сотовой связи. E–mail: bykovmu@ya.ru

*Кущев Сергей Сергеевич* – кандидат технических наук, начальник кафедры. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: методы и системы защиты информации. E–mail: serkser@list.ru

*Перегудов Максим Анатольевич* – кандидат технических наук. Докторант. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: защита информации, моделирование сетей связи. E–mail: maxaperegudov@mail.ru

Адрес: 394064, Россия, г. Воронеж, ул. Ст. Большевиков, д. 54А.

---

# Authentication in Cellular Networks: Evolution, Review of Security Methods and New Vulnerabilities

A. A. Boyko, M. Yu. Bykov, S. S. Kuschev, M. A. Peregudov

***Task Statement****: The vast majority of attacks on cellular networks begin with the exploitation of vulnerabilities in their authentication procedures, allowing attackers to intercept, view, and modify user information. Numerous studies focus on the security of cellular network standards such as AMPS, NMT, GSM, UMTS, LTE, and 5G. However, despite in-depth theoretical research, these studies are fragmented and do not enable a comprehensive view of the development of authentication procedures in cellular networks from the first to the current generation, as well as the methods for exploiting these procedures' vulnerabilities (the so-called IMSI catchers). The aim of this work is to analyze the evolution of authentication procedures in cellular networks to identify patterns in the origins of these vulnerabilities for forecasting the further development of interception devices and creating effective countermeasures.* ***Methods used****: systems analysis method, method for generating cyber-attacks on telecommunications equipment.* ***Novelty****: based on the systematization of existing knowledge using the method of generating cyber-attacks on telecommunications equipment, new, previously unexplored potential vulnerabilities in authentication procedures of various generations of cellular networks have been identified.* ***Result****: the need to improve the authentication procedure in cellular networks, taking into account identified vulnerabilities, has been identified, revealing a contradiction in practice: the demand for measures that eliminate vulnerabilities in the authentication procedure and the lack of such measures.* ***Practical significance****: the result of this work serves as a motivating factor to improve the scientific-methodological apparatus for assessing the effectiveness of countering existing vulnerabilities and establishes the foundation for developing effective means of protecting mobile device information, which will minimize the risks associated with cyber-attacks and ensure the protection of critical information during storage, transmission, and processing.*

***Key words:*** *mobile communication security, false base stations, IMSI-catcher, StingRay, GSM, UMTS, LTE, 5G.*

## Information about Authors

*Aleksey Aleksandrovich Boyko* – Doctor of Engineering Sciences, Associate Professor. Lecturer. Zhukovsky and Gagarin Military Aviation Academy. Field of research: methods and systems of information protection, methods of assessing the effectiveness of complex systems. E–mail: albo@list.ru

*Mikhail Yuryevich Bykov* – Postgraduate. Zhukovsky and Gagarin Military Aviation Academy. Field of research: information security of cellular communication systems. E-mail: bykovmu@ya.ru

*Sergey Sergeyevich Kuschev* – Ph.D. of Engineering Sciences. Head of the Department. Zhukovsky and Gagarin Military Aviation Academy. Field of research: methods and systems of information protection. E-mail: serkser@list.ru

*Maxim Anatol'evich Peregudov* – Ph.D. of Engineering Sciences. Doctoral Candidate. Zhukovsky and Gagarin Military Aviation Academy. Field of research: information security, modeling of radio network. E-mail: maxaperegudov@mail.ru

Address: Russia, 394064, Voronezh, Old Bolsheviks Street, 54A.