УДК 381.3

Применение технологии Embedded SIM для обеспечения информационной безопасности в сетях сотовой связи

А. С. Шелков, м. т. н., инженер УП «Велком» (220030, г.Минск, ул. Интернациональная, 36-2). E-mail: asshelkou@gmail.com

Аннотация. В статье рассматриваются общая классификация угроз информационной безопасности сетей операторов сотовой связи, основные угрозы безопасности абонентским устройствам в сетях операторов сотовой связи, технология embedded SIM и возможность ее использования для обеспечения безопасности абонентских устройств. Проанализирована статистика по зарегистрированным случаям реализации угроз информационной безопасности на абонентских устройствах. Предложена высокоуровневая архитектура системы защиты абонентских устройств с использованием технологии eSIM.

Ключевые слова: информационная безопасность, оператор сотовой связи, провайдер связи, вредоносное ПО, fraud, eSIM.

Application of Embedded SIM Technology to Provide Information Security in Cellular Networks

A. S. Shelkov, Master of Technical Sciences, engineer of UE Velcom (220030, Minsk, Internacional'naja str., 36-2).
E-mail: asshelkou@gmail.com

Abstract. The article describe the general classification of threats to information security of cellular operators' networks, the main security threats to subscriber devices in the networks of cellular operators, embedded SIM technology and the possibility of using this technology to ensure the security of subscriber devices. The statistics on the registered cases of the implementation of threats to information security on subscriber devices is analyzed. A high-level architecture for the protection of subscriber devices using eSIM technology is proposed.

Key words: information security, mobile network operator, connection provider, malware, fraud, eSIM.

Введение. Сети провайдеров связи (телекоммуникационных операторов) представляют собой сложную связанную систему, задача которой — предоставление услуг связи абонентам для получения денежной прибыли. Обеспечение информационной безопасности подобной структуры — сложная задача, требующая структурированного подхода.

Основная часть. Схематическая структура компонентов сети оператора сотовой связи с разбиением на уровни изображена на рис. 1.

Основные виды угроз информационной безопасности в телекоммуникационных системах:

1) угроза целостности информации;
2) угроза конфиденциальности информации;
3) угроза доступности информации;
4) угроза достоверности информации.

Все эти типы угроз можно рассматривать по отношению к компонентам и каналам связи между ними в сети оператора сотовой связи. В теории осуществлением информационной безопасности объектов связи и каналов связи между этими объектами должны заниматься технические специалисты провайдера связи, получая указания и рекомендации от специалистов по информационной безопасности.

В данной схеме наиболее уязвимым местом является уровень доступа к сети — абонентские терминалы (устройства), причём злоумышленники могут нанести ущерб пользователям и сети провайдера легально и без применения дорогостоящего оборудования. Технические специалисты провайдера связи не могут и не имеют право вести наблюдение за абонентскими устройствами. Это приводит к тому, что та часть абонентов, которая не следует рекомендациям по информационной безопасности, может пострадать от следующих типов угроз:

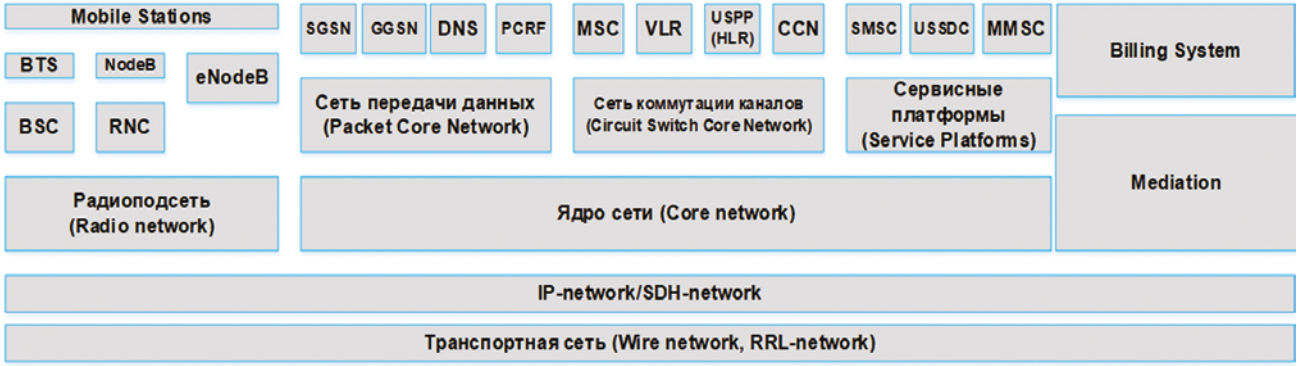

Рис. 1. Структура сети оператора сотовой связи

1) вредоносное программное обеспечение;

2) спам в сетях провайдера связи;

3) мошенничество в сетях связи (fraud).

Согласно статистическому отчёту компании «Kaspersky Lab» [1] ситуация за последний год такова:

1) увеличилось количество пользователей, атакованных при помощи вредоносного ПО «TROJAN-BANKER», распространяемого с использованием SMS-спама (рис. 2);

2) во втором квартале 2017 года «Лаборатория Касперского» обнаружила 1 319 148 установленных экземпляров вредоносного ПО, что почти столько же, сколько в двух предыдущих кварталах (рис. 3);

3) наблюдается рост зарегистрированных случаев мошенничества в сетях связи (fraud) (рис. 4) [1].

Для идентификации (а также для аутентификации и авторизации) операторами сотовой связи традиционно используются модули идентификации абонента (SIM). Этот модуль представляет собой миниатюрный чип, в котором содержится международный идентификатор мобильного абонента (IMSI), ключи шифрования и фиксированный объём памяти и вычислительной мощности. В этом модуле могут работать различные апплеты. Через модуль SIM абонент привязан к конкретному оператору связи и, как правило, абонентский терминал поддерживает 1–2 слота для SIM-карты.

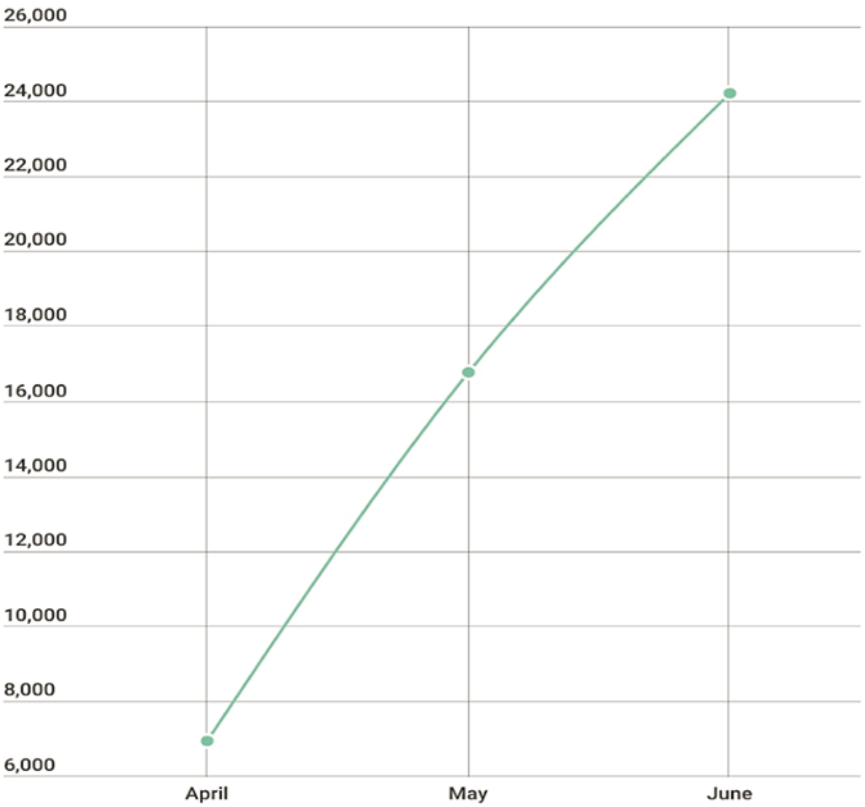

Рис. 2. Количество пользователей, атакованных при помощи вредоносного ПО «TROJAN-BANKER»

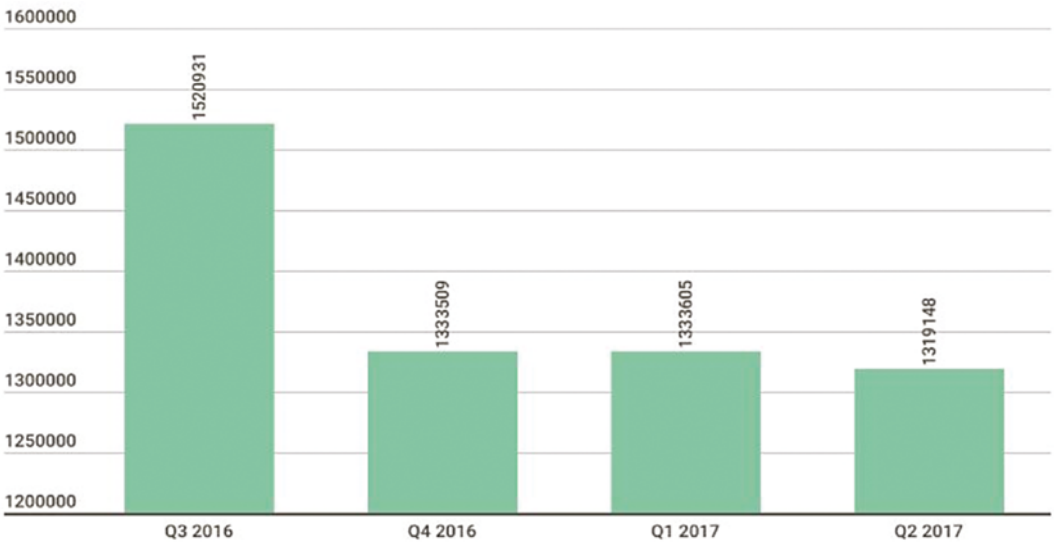

Рис. 3. Количество установленных экземпляров вредоносного ПО

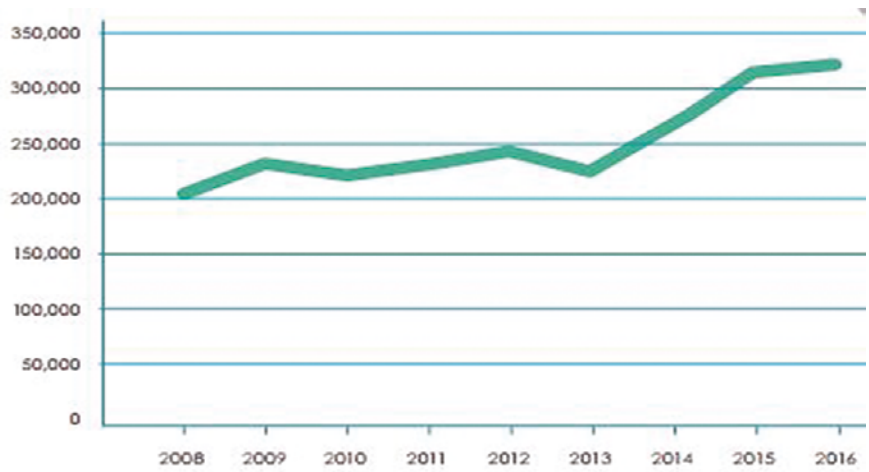

Рис. 4. Количество зарегистрированных случаев мошенничества в сетях связи (fraud)

Летом 2014 года ассоциацией GSM было заявлено о начале создания спецификации для технологии embedded SIM. Основная суть данной технологии — использование в качестве SIM встроенного в абонентский терминал микрочипа, позволяющего абоненту переключаться между различными операторами связи путём загрузки данных SIM в этот микрочип. В 2017 году принята действующая версия спецификации архитектуры системы 2.1 [2].

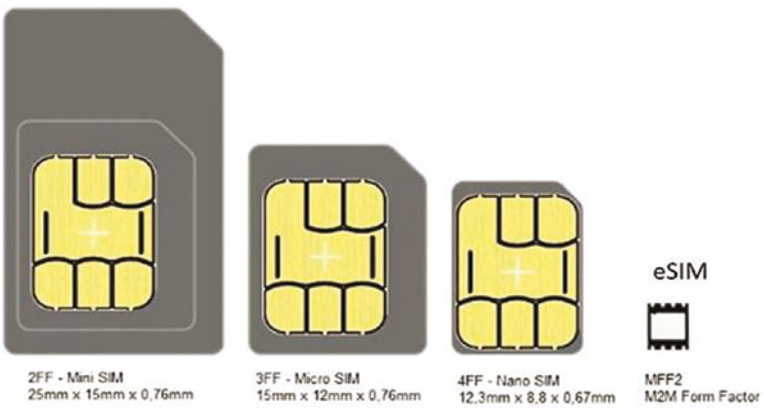

Рис. 5. Форм-факторы SIM и eSIM

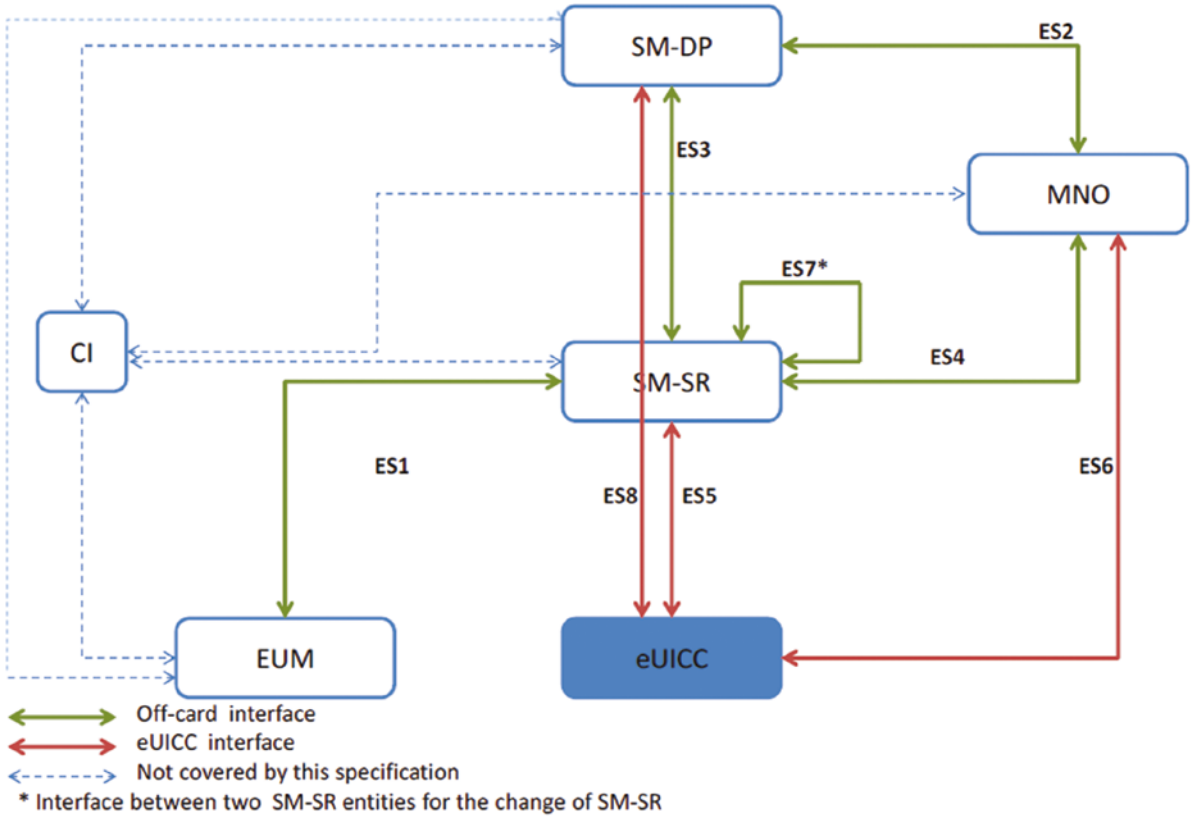

Рис. 6. Функциональная архитектура eSIM (eUICC)

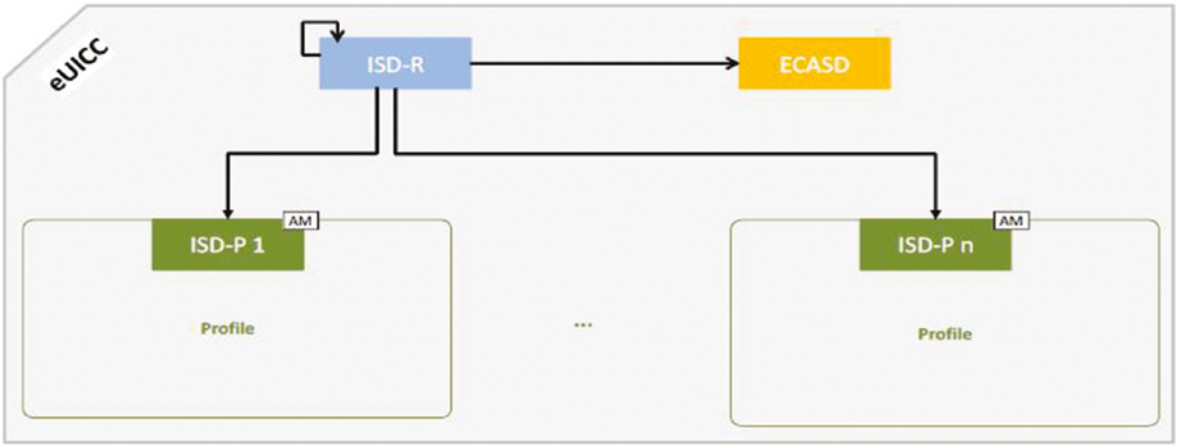

Рис. 7. Программная архитектура eSIM (eUICC)

Фукциональная схема технологии eSIM изображена на рисунке 6.

Согласно спецификации оператор сотовой связи (MNO) сможет загрузить профиль SIM в чип eSIM. На рисунке 7 изображена программная архитектура чипа eSIM.

Программная архитектура eSIM подразумевает наличие нескольких профилей (profile), которые программным образом представляют собой SIM оператора сотовой связи. Структура профиля схематично показана на рисунке 8.

Абонент может загрузить профиль любого провайдера связи, который поддерживает технологию eSIM. Загрузка профиля осуществляется согласно схеме на рисунке 6 [3].

Загруженный в чип eSIM профиль абонента может иметь свои собственные приложения (application).

Разработка профиля защиты абонентского устройства может быть основана на возможности провайдера связи внедрить в профиль eSIM специальное приложение, которое сможет

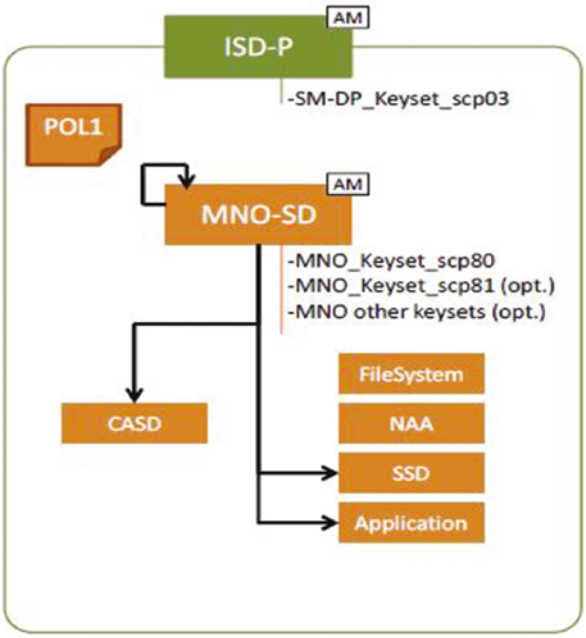

Рис. 8. Структура профиля абонента

выполнять функции антивируса, детектора мошенничества в сетях связи, а также выполнять функции анализатора качества предоставляемых сервисов. При этом провайдер связи может организовать централизованный контроль, сбор и анализ статистических показателей данного приложения при помощи специальной платформы, взаимодействующей с профилями eSIM через OTA. Схематично точки анализа изображены на рисунке 9.

Данное приложение должно сканировать работу абонентского устройства на предмет аномальной активности:

1) изучение корректности служебных сообщений устройства в сети оператора связи;

2) анализ на предмет наличия вредоносного ПО;

3) анализ активности абонента;

4) измерение параметров связи.

Полученные данные должны будут передаваться на специальную платформу, у которой должна быть необходимая вычислительная мощность, чтобы:

1) проанализировать полученные данные;

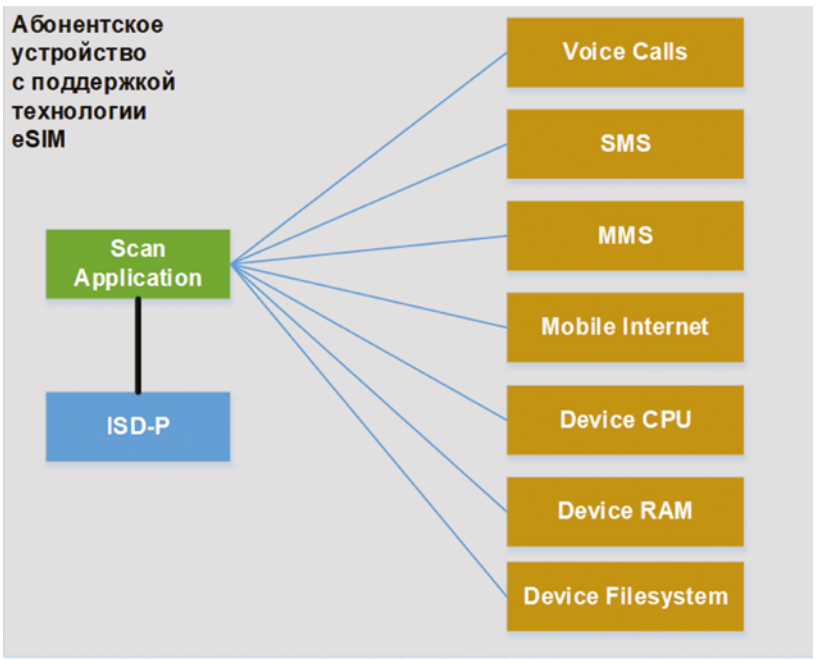

Рис. 9. Схема взаимодействия защитного приложения с компонентами абонентского устройства

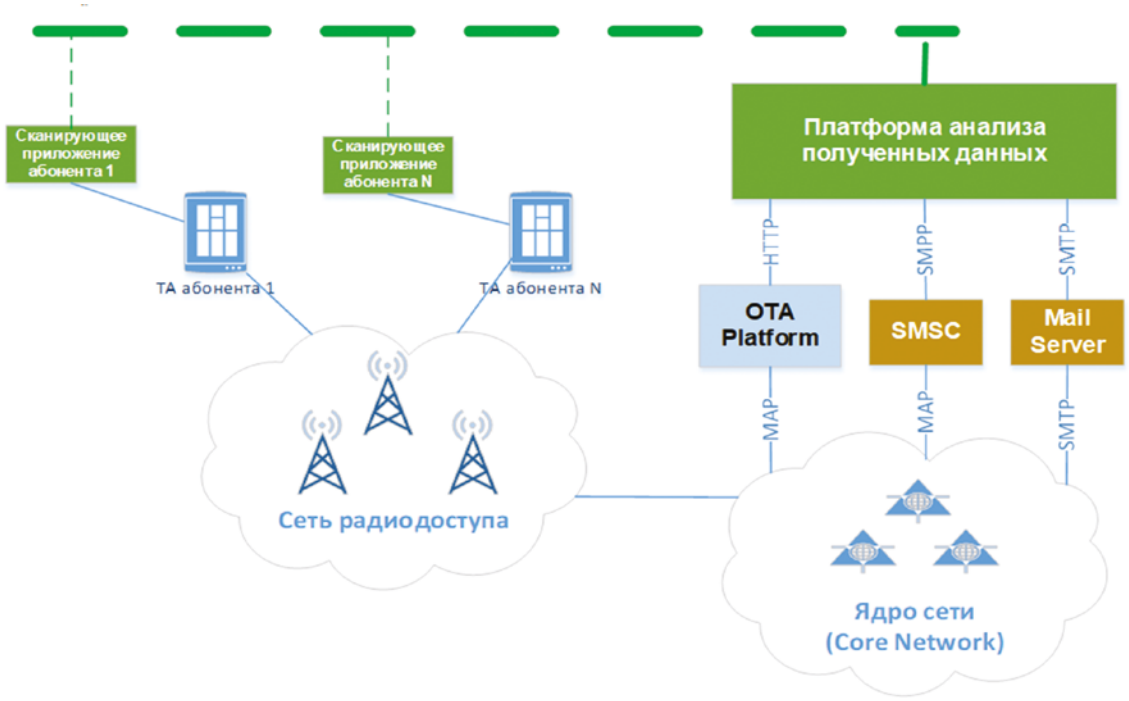

Рис. 10. Схема интеграции платформы анализа в сеть мобильного оператора

2) обнаружить реальные и потенциальные угрозы;

3) сформировать отчёт по каждому абонентскому устройству и отправить каждому абоненту уведомление, если имеется реальная или потенциальная угроза безопасности.

Таким образом, согласно схеме интеграции платформы анализа в сеть мобильного оператора, изображенной на рисунке 10, специальное приложение будет осуществлять сканирование компонентов на абонентских устройствах и передавать полученную информацию на платформу анализа, используя методы OTA (Over-the-Air). Платформа будет анализировать полученные данные и рассылать результаты анализа через SMS и email абонентам и специалистам информационной безопасности мобильного оператора.

Заключение. Полученная схема позволит оператору сотовой связи участвовать в обеспечении информационной безопасности абонентских устройств, что позволит повысить лояльность абонентов и репутацию мобильного оператора на рынке услуг связи.

Список литературы

1. IT threat evolution Q2 2017. Statistics [Electronic resource] / Kaspersky lab. – Mode of access: https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/. – Date of access: 28.09.2017.
2. SGP.02 v3.2 — Remote Provisioning Architecture for Embedded UICC Technical Specification [Electronic resource] / GSMA. Mode of access: https://www.gsma.com/newsroom/all-documents/sgp-02-v3-2-remote-provisioning-architecture-for-embedded-uicc-technical-specification/. – Date of access: 28.09.2017.
3. Remote Provisioning Architecture for Embedded UICC technical specification. Version 3.2: official document SGP.02. – GSM Association, 2017. – 309 p.

References

1. IT threat evolution Q2 2017. Statistics. Available at: https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/ (accessed 28.09.2017).
2. SGP.02 v3.2 — Remote Provisioning Architecture for Embedded UICC Technical Specification. Available at: https://www.gsma.com/newsroom/all-documents/sgp-02-v3-2-remote-provisioning-architecture-for-embedded-uicc-technical-specification/ (accessed 28.09.2017).
3. Remote Provisioning Architecture for Embedded UICC technical specification. Version 3.2: official document SGP.02. GSM Association, 2017. 309 p.

Статья поступила: 11.12.2017 г.