ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ ОПЕРАТОРА СОТОВОЙ СВЯЗИ

Коновалов С.Ю.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Современный мир невозможно представить без мобильной связи. Многие пользователи банковских приложений, интернет-магазинов и других интернет-услуг хорошо знакомы с многочисленными SMS сообщениями с одноразовыми кодами подтверждения. Однако, безопасность данного способа аутентификации стоит под большим вопросом. Также существуют и другие способы, которыми пользуются злоумышленники.

В последние годы проведение успешных атак оставалось на достаточно высоком уровне. Это доказывает диаграмма, приведенная на рисунке 1.

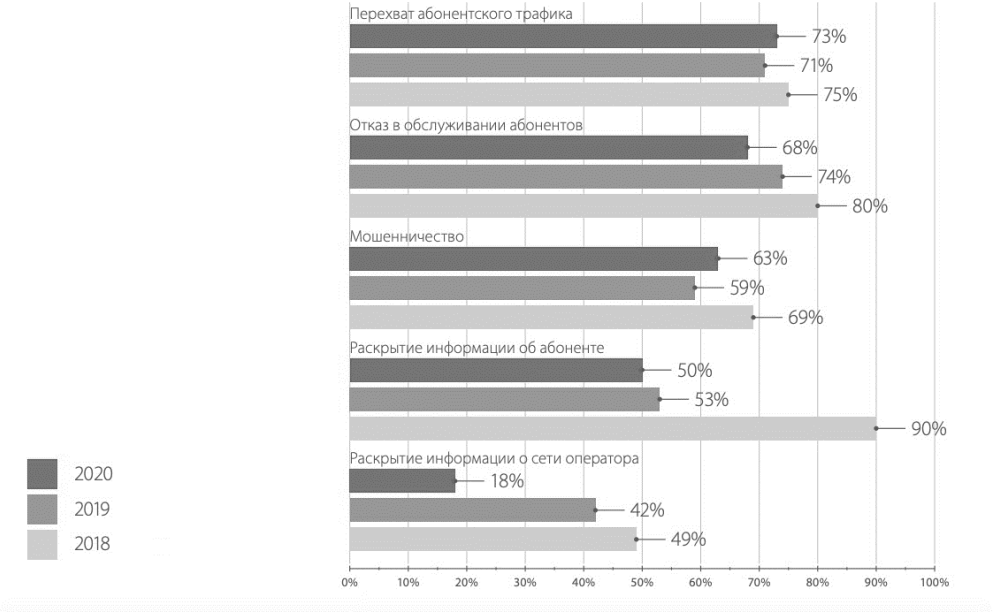

Рисунок 1 – Доли успешных атак по типам угроз

Для противостояния многочисленным атакам злоумышленников необходимо внедрять дополнительные системы обеспечения безопасности. Они должны учитывать специфику современных атак и быть готовыми расширить свою функциональность при необходимости.

Для защиты от атак на инфраструктуру мобильной сети необходимо использовать рекомендации:

– провести проверку текущего оборудования и сменить конфигураций по умолчанию, такие же действия проводить с новым оборудованием;

– настроить системы для непрерывного мониторинга трафика

пользователей в режиме реального времени;

– на основе проведенного мониторинга устанавливать правили фильтрации ложных и мошеннических запросов;

– проводить периодический аудит информационной безопасности элементов инфраструктуры;

– установить дополнительны системы защиты для особенно уязвимых устройств и систем;

– настроить резервирование каналов связи и систем обработки информации.

Для реализации рекомендаций по защите инфраструктуры мобильной сети разработана ее модифицированная схема, которая представлена на рисунке 2.

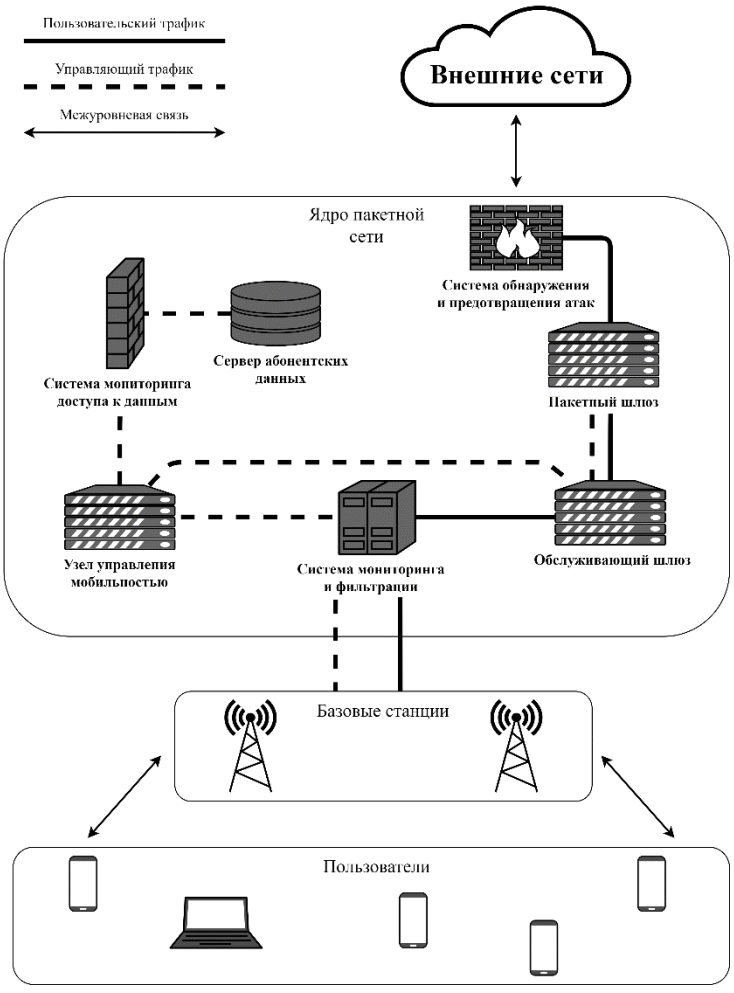

Рисунок 2 – Модифицированная схема инфраструктуры мобильной сети