Локальный защищенный оператор связи

решение по защите связи для государственных объектов

Угрозы, связанные с уязвимостями современных систем связи

Существует несколько глобальных проблем, которые делают использование мобильных технологий в государственных зданиях потенциально опасными с точки зрения утечки конфиденциальной и секретной информации:

01 Несанкционированный пронос телефона сотрудниками и посетителями:

- Фото служебной информации
- Диктофонные записи служебных разговоров

02 Неконтролируемые звонки сотрудников в здании, что ведет к утечке информации

03 Пронос вирусов на телефонах с USB-разъемом для заражения служебных компьютеров

04 Методы разведки на основе открытых источников могут использоваться зарубежными спецслужбами для получения ценных сведений на основе обобщения открытой информации передвижения сотрудников и их карт звонков

Угрозы, связанные с уязвимостями современных систем связи

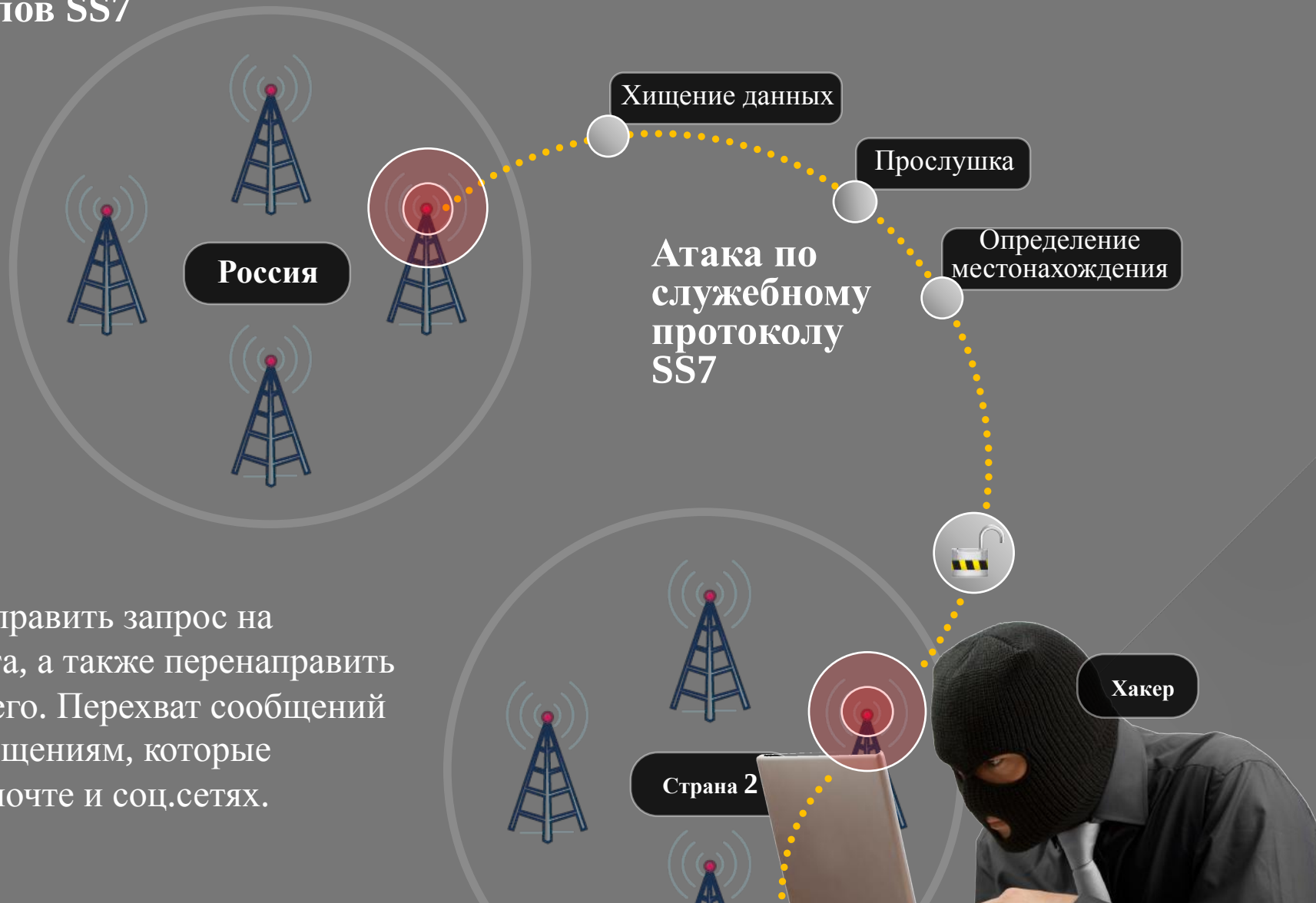
05

Атаки через стек протоколов SS7

SS7- стек служебных телефонных протоколов, используемых для настройки соединений всеми мировыми операторами связи.

Основная уязвимость SS7 заключается в том, что любой получаемый сетью запрос считается легитимным.

Хакер с доступом к SS7 может отправить запрос на местонахождение любого абонента, а также перенаправить звонок атакуемого и прослушать его. Перехват сообщений позволяет получить доступ к сообщениям, которые используются для авторизации в почте и соц.сетях.



Предлагаемое решение по защите связи для государственных объектов: организация локального защищенного оператора связи

Мобильный оператор внутри выделенного здания

Мобильный оператор сосредоточен исключительно внутри здания, все звонки между абонентами совершаются внутри здания без выхода на сотовых операторов страны, что крайне важно с учетом того, что сети мобильного оператора имеют в том числе иностранный капитал.

Зона, изолированная от внешнего оператора и как следствие SS7 атак

Соты локального защищенного оператора располагаются внутри здания

Предлагаемое решение по защите связи для государственных объектов: организация различных политик для мобильных устройств на объекте

Различные политики для разных комнат

Защищенный оператор по настройкам офицера безопасности может отключать у пользователей мобильных устройств из белых списков в разных комнатах в зависимости от настроек различные сервисы: GSM-связь, камера и диктофон на устройствах, SMS-переписка. Отключение проводится с использованием Device Mobile Management клиента, установленного на телефоны белого списка.

Возможность снятия ограничений для определенных лиц из белого списка

Предлагаемое решение по защите связи для государственных объектов: спец.лифт и категоризация этажей

Зона, изолированная от SS7 атак

Разные категории этажей с разными уровнями доступа

При остановке спец.лифта на этаже служба охраны на специальном пано индикаторов видит все телефоны посетителей и определяет, находятся ли они в белом или черном списках

Спец.лифт, оборудованный системой считывания идентификаторов телефонов, позволяет быстро идентифицировать людей в лифте по их телефонам

Предлагаемое решение по защите связи для государственных объектов: поиск людей на прилегающих к зданию территориях

Локальный защищенный оператор связи

На территории, прилегающий к объекту с защищенным оператором, может быть установлена периметровая охрана, позволяющая обнаружить телефоны из черного списка на прилегающей территории

Зона защищенного оператора

На прилегающей территории защищенные звонки могут осуществляться в специальных беседках

Сканнер 2G, 3G, 4G частот

Предлагаемое решение по защите связи для государственных объектов: соединение распределенных территориальных объектов

Здание локального защищенного оператора

Страна 1

Шифрованный канал через сеть Интернет

Оператор может покрыть два здания в разных странах

Здание локального защищенного оператора

Страна 2

Предлагаемое решение по защите связи для государственных объектов: интеграция с открытыми операторами связи

Локальный защищенный оператор может подключаться к внешним операторам через специальный защищенный шлюз, что сделает возможным внешние звонки согласно установленным политикам

Хранилище записей переговоров в оцифрованном виде с функцией поиска по ключевым словам

Использование криптогарнитуры для подключения к защищенному оператору из внешнего контура по шифрованному каналу

Звонок внутри защищенного оператора

Сервер

Открытая связь