УДК 342.723

УГРОЗЫ БЕЗОПАСНОСТИ В СЕТЯХ СОТОВОЙ СВЯЗИ

И. Д. Цуранова

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

Научный руководитель Н. С. Ищенко

Выявлены потенциальные риски для беспроводных сетей, изучены возможные уязвимости, законодательство в данной сфере и предложены контрмеры для повышения уровня защиты систем от возникающих проблем безопасности.

Ключевые слова: угрозы безопасности, атака, фишинг, конфиденциальность, персональные данные, способы защиты, мобильная связь, шифрование, правонарушитель.

SECURITY THREATS IN CELLULAR NETWORKS

I. D. Tsuranova

Sukhoi State Technical University of Gomel, Republic of Belarus

Scientific supervisor N. S. Ishchenko

The paper identifies potential risks for wireless networks, examines possible vulnerabilities, legislation in this area, and suggests countermeasures to increase the level of protection of systems from emerging security problems.

Keywords: security threats, attack, phishing, confidentiality, personal data, methods of protection, mobile communication, encryption, offender.

Беспроводные сети развертываются в государственных и образовательных учреждениях, в медицинских организациях, местах отдыха, на предприятиях, в общественных местах и т. д. Активно укрепляют свои позиции различные беспроводные технологии, такие как GSM, 3G, GPRS, Bluetooth, особо перспективно развитие беспроводных локальных сетей (WLAN). Так, повышение степени комфортности жилья путем объединения всех его структур и объектов – основная идея создания Интернета вещей [5]. Наиболее высокий рост беспроводных технологий, несмотря на то, что существует большое количество индивидуальных пользователей, продолжает наблюдаться в организациях [4, 5]. Компания Positive Technologies провела мониторинг сетевой активности в 60 компаниях, в 93 % организаций были получены данные о подозрительной сетевой активности: сокрытии трафика, получение данных о пользователях, парольной политике с контроллера домена, а также высокий уровень попыток удаленного запуска процессов. Проведение исследования уязвимостей и угроз безопасности поможет повысить уровень безопасности беспроводных сетей и защитить конфиденциальную информацию компании от внешних угроз.

Таким образом, проведение исследования уязвимостей и угроз безопасности является весьма актуальным для повышения степени защиты информационных систем и технологий.

К основным угрозам безопасности беспроводного стандарта можно отнести: нарушение конфиденциальности и аутентичности передаваемой информации, целостности передаваемых данных, контроль доступа к точке доступа, а также нарушение доступности (перехват трафика с последующим нарушением функционирования

канала связи) [4, 5]. Вопрос обеспечения конфиденциальности возможно решить с помощью шифрования сетевого трафика. Для решения данной проблемы в сетях Wi-Fi применяются протоколы защиты: WEP – протокол шифрования, основанный на алгоритме шифрования RC4 (Rivest Chipher 4) с 40- и 104-битовым ключом, который складывается со сгенерированным вектором инициализации. Несмотря на то, что WEP является наиболее старым механизмом защиты, и он может легко быть взломан, некоторые организации все еще используют его, так как они не могут использовать WPA2 из-за ограничений старых устройств. Для протоколов шифрования WPA и WPA2 характерно использование криптографического алгоритма AES. Данные протоколы являются более надежными механизмами защиты, особенно WPA2, который считается наиболее безопасным за счет использования алгоритма AES совместно с алгоритмом блочного шифрования CCMP. Однако, даже используя эти механизмы, возможны атаки на беспроводные сети, поэтому дополнительные меры безопасности должны использоваться, такие как ограничение доступа к сети только для авторизованных пользователей и использование VPN для дополнительной защиты данных [4, 5]. Также последней разработкой стал протокол шифрования WEP3, сохранивший алгоритм шифрования AES, но с заменой CCMP на GCMP. К тому же добавлено использование технологии SEA (Simultaneous Authentication of Equals). В вопросах безопасности важную роль играет целостность информации, в рамках беспроводных сетей этого можно достигнуть с помощью проверки контрольной суммы (CRC- 32) с шифрованием передаваемых данных алгоритмом RC4. Существует ряд методов борьбы с уязвимостями и угрозами беспроводного протокола. Обновление программного обеспечения: вендоры выпускают обновления для устройств, которые исправляют уязвимости, поэтому важно регулярно обновлять программное обеспечение на всех устройствах, использующих беспроводную сеть. 2. Применение безопасных настроек: при настройке беспроводной сети необходимы пароли и шифрование данных. 3. Использование WPA2: WPA2 является наиболее безопасным протоколом для защиты беспроводной сети, поэтому его следует использовать вместо устаревших протоколов, таких как WEP. 4. Применение сетевых устройств с поддержкой обнаружения ипредотвращения атак: некоторые современные маршрутизаторы и точки доступа обладают функцией обнаружения и предотвращения атак, что может снизить уровень угроз для беспроводной сети. 5. Использование VPN: виртуальная частная сеть (VPN) позволяет шифровать данные, передаваемые через беспроводную сеть, что делает их невозможными для перехвата правонарушителями. 6. Физическая защита устройств: защита беспроводных устройств от физического доступа также является важным мероприятием, так как правонарушители могут получить доступ к устройствам и использовать их для атак на беспроводную сеть. 7. Использование сетевых анализаторов: сетевые анализаторы могут использоваться для обнаружения несанкционированного доступа и атака на беспроводную сеть. В целом, комбинация этих методов может помочь защитить беспроводную сеть от уязвимостей и угроз. Однако важно понимать, что безопасность беспроводной сети – это является непрерывным процессом и требует постоянного обновления и улучшения мер защиты [4, 5]. Безопасность беспроводной сети является важным вопросом и требует постоянного внимания со стороны пользователей и администраторов сети. Необходимо регулярное обновление программного обеспечения и использование современных методов защиты, что, безусловно должно быть отражено в нормах права.

Мобильный телефон является неотъемлемой частью жизни любого современного человека. Пользователи, находясь практически в любом месте земного шара,

могут использовать различные возможности своих телефонов: отправлять друг другу SMS-сообщения, осуществлять телефонные вызовы, просматривать и редактировать документы любых форматов, получать доступ в Интернет. Многие хранимые и передаваемые данные являются конфиденциальными. Развитие мобильных технологий ведет к большому количеству различных атак на мобильные устройства. Основные возможности правонарушителя – это подслушивание разговора, определение местоположения человека, перехват SMS для доступа к мобильному банку, а также проведение спам-атак, которые можно рассматривать как DDos-атаки. Эти угрозы безопасности возможны в том случае, если правонарушителю известен номер телефона потенциального потерпевшего. Самой простой атакой на телефон является спам-атака. SMS и DDos-атаки широко применяется правонарушителями для доставки неудобств частным лицам и нанесения морального ущерба. Спам-атака на мобильное устройство – постоянные звонки или сообщения, которые приходят к потерпевшему на телефон. Основным методом при такой атаке является ПО SMS-Bomber. Постоянный поток сообщений может нести в себе рекламу, новости, призыв к действию или содержать ссылки на вирусы. Спам сообщений – непрерывный поток SMS с бессмысленным содержанием, угрозами, рекламным содержанием или вирусами. Потенциальная жертва будет получать их с различных телефонных номеров. Опасности подвергаются пользовательские данные, настройки и прочая конфиденциальная информация. Если DDos нападение будет успешным, то правонарушители могут получить доступ к страницам в социальных сетях, к платежным средствам, e-mail и другой информации потенциальной жертвы. Вытекающей атакой из DDos-атаки может быть фишинг. В сообщениях могут содержаться ссылки, через которые пользователь самостоятельно скачает себе вредоносное ПО-вирусы, перейдя по этой ссылке, и может попасть на фишинговую страницу, через которую произойдет утечка персональных данных. К вирусам можно отнести программы-вымогатели, которые работают по принципу вируса WannaCry. Сюда же можно отнести вредоносную программу, которая заражает девайс, превращая его в часть ботнета, и иное вредоносное ПО с помощью которого злоумышленник может получить контроль над вашим устройствам. Юридический аспект данного вопроса урегулирован нормами Основного закона (ст. 28 Конституции) и уголовного кодекса Республики Беларусь (УК РБ – ст. 203–204; гл. 31 Преступления против компьютерной безопасности).

Каждый имеет право на защиту от незаконного вмешательства в его частную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство (ч. 1), государство создает условия для защиты персональных данных и безопасности личности и общества при их использовании (ч. 2 ст. 28 Конституции). Уголовная ответственность предусмотрена за следующие преступления: нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений (ст. 203); незаконные действия в отношении информации о частной жизни и персональных данных (ст. 203^1); несоблюдение мер обеспечения защиты персональных данных (ст. 203^2); отказ в предоставлении гражданину информации (ст. 204); хищение имущества путем модификации компьютерной информации (ст. 212); несанкционированный доступ к компьютерной информации (ст. 349); уничтожение, блокирование или модификация компьютерной информации (ст. 350); неправомерное завладение компьютерной информацией (ст. 352); разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (ст. 354); нарушение правил эксплуатации компьютерной системы или сети (ст. 355) и др.

Главным вопросом остается способ защиты от такого рода атак. Существует несколько способов защиты от спам-атаки: не оставлять свой номер на сайтах и нигде не публиковать его; если атака проводится с одного номера, то можно заблокировать данный номер, добавив его в «черный список»; если атака проводится с различных номеров, то решением в данной ситуации будет блокировка дозвонов всех номеров, не входящих в телефонную книгу (данное решение не подходит для лиц, ведущих бизнес); также рекомендуется устанавливать в начале дозвона, до соединения с оператором, проверку на ботов – голосовое сообщение с приветствием, например: «Здравствуйте, вас приветствует компания « Аврора», для получения справки нажмите 1, для связи с оператором жмите 0»; использовать сторонние приложения для определения номера и блокировки нежелательныхзвонков, такие как Whoscall, Show Caller и Hiya.

Способы защиты от фишинга и следующим за ним вредоносных программ: основной способ защиты от фишинга – пользователь не должен переходить по ссылкам, пришедшим ему в спам-сообщениях при DDos-атаках; установка на мобильное устройство антивирусной программы; необходимость регулярного обновления программное обеспечения устройства и приложений. Среди угроз информационной безопасности мобильной связи можно также выделить угрозу определения текущего местоположения абонента. С помощью специальных сообщений-утилит правонарушитель будет использовать недостатки, связанные с отсутствием фильтрации неиспользуемых сигнальных сообщений. Данное сообщение протокола MAP используется при входящем голосовом вызове и служит для запроса маршрутной информации для локализации вызываемого абонента. При нормальном режиме функционирования это сообщение должно передаваться только между элементами своей сети. Используя данный метод, правонарушитель, может определить текущее местоположение абонента. Примером таких сигнальных сообщений являются ProvideSubscriberInfo, SendRoutingInfo, AnyTimeInterrogation и SendRoutingInfoForSM. Самым эффективным способом нарушителей для получения информации о местонахождении абонента является метод ProvideSubscriberInfo, который используется для получения информации о местоположении абонента в интересах различных сервисов. Угроза прослушивания входящих звонков абонента основана на принципе методов подмены перевода трафика на другой коммутатор и манипуляции с переадресацией. Атакующий может заменить в профиле значение платформы для тарификации вызовов на адрес своего оборудования. В момент исходящего вызова мобильный коммутатор отправит запрос на продолжение вызова на указанный правонарушителем адрес. Правонарушитель должен отправить директиву на перенаправление вызова на подконтрольную ему АТС, затем перекоммутировать трафик на вызываемого абонента.

Следовательно, разговор между двумя абонентами пойдет в открытом виде через АТС, полностью подконтрольную атакующему. В случае перенаправления номера на фальшивый номер оплата данного вызова ляжет на абонента. Основным инструментом злоумышленника в данном случае является метод InsertSubscriberData. Данная угроза реализуется вследствие «дыры» в архитектуре сети, связанной с отсутствием проверки реального местоположения абонента. Для перехвата же SMS-сообщений нарушители используют утилит UpdateLocation, с помощью которого происходит регистрация абонента в фальшивой сети, после данного действия все сообщения будут приходить на адрес, указанный атакующим. Все эти действия правонарушителя противоречат Конституции Республики Беларусь (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г., 17 октября 2004 г. и 27 февраля 2022 г).

Таким образом, в Беларуси гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи [3]. Ответственность за данное деяние возникает в соответствии с УК РБ. Право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений является существенным условием неприкосновенности личной жизни и одной из объективных составляющих основного правопорядка. Отсюда можно сделать вывод, что действия атакующего нарушает нормы конституционного права. Необходимо реализовать фильтрацию таким образом, чтобы отсекались лишь нежелательные сообщения, используемые в рамках атак. Для этого рекомендуется внедрять дополнительные средства защиты, например, программно-аппаратные комплексы класса IDS, такие как ПАК ViPNet IDS NS. Подобные системы не влияют на трафик сети, однако при этом позволяют выявлять действия нарушителя и определять настройки фильтрации сообщений, необходимые для предотвращения атак. Также абонента может самостоятельно защитить себя от всех видов угроз, используя: сторонние приложения, например EAGLE Security, Spyware Detecror (сканер шпионских программ); комбинации цифр и спецзнаков. Самым эффективным способом защиты будет комбинация всех названных методов. Однако не каждый оператор связи, особенно обладающий сравнительно небольшой абонентской базой, может обеспечить такой аудит на должном уровне. В таких случаях, необходимо регулярно проводить аудит сетей мобильной связи с привлечением сторонних специализированных организаций. Это позволит объективно определить текущий уровень защищенности, выявить существующие угрозы безопасности и минимизировать существующие риски, приняв своевременные меры по устранению уязвимостей. Мобильная связь – важнейшее средство коммуникации в современном мире. Одновременно у мобильной связи есть один значительный недостаток: передача данных идет в радиоэфире, где эта информация может быть перехвачена. Серьезность же последствий такой утечки сведений может быть огромна, в зависимости от уровня конфиденциальности этой информации. Исходя из вышеизложенного, можно сделать вывод, что телекоммуникационные компании используют различные меры защиты, но их явно недостаточно, чтобы компенсировать весь спектр методов, которые могут применять потенциальные нарушители. Абоненты даже крупных операторов связи не защищены от несанкционированного прослушивания звонков, перехвата SMS-сообщений, перенаправления вызовов и хищения денежных средств со счета, определения текущего местонахождения абонента.

Литература

1. Конституция Республики Беларусь 1994 года (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г., 17 октября 2004 г. и 27 февраля 2022 г.). – URL: https://ск:etalonline.by/document/?regnum=v19402875.
2. Ищенко, Н. С. Конституционное право : пособие для слушателей специальностей переподготовки 1-24 01 71 «Правоведение» и 1-24 01 72 «Экономическое право» заоч. формы обучения / Н. С. Ищенко ; М-во образования Респ. Беларусь, Гомел. гос. техн. ун-т им. П. О. Сухого, Ин-т повышения квалификации и переподготовки, каф. соц.-гуманитар. и правовых дисциплин. – Гомель : ГГТУ им. П. О. Сухого, 2022. – 506 с.
3. Ищенко, Н. С. Право неприкосновенности личности в Республике Беларусь / Н. С. Ищенко. – Минск : Тесей, 2005 – 176 с.
4. Уязвимость в протоколе SS7 уже несколько лет используют для перехвата SMS и обхода двухфакторной аутентификации // Хабр. – URL: https://habr.com/ru/post/403649/ (дата обращения: 05.04.2025).
5. Kartsan, I. N. Koncepcija razvitija mezhsputnikovoj lazernoj svjazi / I. N. Kartsan // Sibirskij ajerokosmicheskij zhurnal. – 2023. – N 24 (2). – P. 247–259. – URL: https://doi.org/10.31772/2712-8970-2023 (дата обращения: 05.04.2025).