Безопасность данных требует их резервирования на разных носителях, что часто игнорируется. Специалисты должны помнить о необходимости распределения данных и защиты компьютеров от перепадов напряжения[1].

Организационные меры включают защиту носителей от кражи, подбор и обучение квалифицированного персонала, а также тестирование помещений на наличие шпионских устройств. Перед передачей информации важно правильно удалять конфиденциальные данные, так как файлы можно восстановить.

Для защиты от несанкционированного доступа используются системы идентификации и надежные пароли, которые необходимо регулярно менять. Эффективны также методы биометрической идентификации, такие как отпечатки пальцев и голосовые характеристики.

Криптография – ключевой метод защиты информации в телекоммуникациях, позволяющий зашифровывать сообщения. Для расшифровки требуется идентифицирующий ключ. Электронная цифровая подпись защищает официальные документы и широко используется в электронном документообороте[2].

Руководство предприятия должно разработать концепцию информационной безопасности и выделить средства на минимальный пакет защитных мер, включая антивирусное ПО, технологии аутентификации и шифрования данных.

Гришин А.Г.,

кандидат юридических наук
Ленинградский областной филиал
Санкт-Петербургского университета МВД России (п. Мурино)

Исследование методов обеспечения безопасности в сетях связи нового поколения

Развитие информационных технологий и повсеместное внедрение беспроводных сетей связи нового поколения ставят новые задачи по обеспечению их информационной безопасности. Уязвимости протоколов связи, сложность криптографических механизмов, большое число пользователей делают беспроводные сети привлекательной мишенью для злоумышленников.

Несанкционированный доступ к конфиденциальной информации, нарушение ее целостности и доступности могут привести к серьезным

[1] Биячуев Т.А. Безопасность корпоративных сетей. СПб: СПб ГУ ИТМО, 2004. 161 с.
[2] Конахович Г. Защита информации в телекоммуникационных системах. М.: МК-Пресс, 2005. 356 с.

последствиям как для отдельных пользователей, так и для организаций и предприятий в целом. Поэтому разработка эффективных методов и средств защиты информации в беспроводных сетях является актуальной научно-технической задачей.

Наиболее распространенными являются угрозы нарушения конфиденциальности передаваемой информации. Из-за открытости радиоканала передачи данных злоумышленник может перехватывать сетевой трафик, находясь в зоне действия сети, и получать несанкционированный доступ к конфиденциальным данным пользователей – логинам, паролям, персональной информации и т.д.

Другой серьезной угрозой является нарушение целостности передаваемых данных. Злоумышленник может внедрять в сетевой трафик ложные пакеты, изменять или удалять передаваемую легальными пользователями информацию. Это может привести к сбоям в работе сетевых приложений, получению пользователями недостоверной информации и т.п.

Угрозы нарушения доступности направлены на срыв нормального функционирования беспроводной сети и отказ в обслуживании легальных пользователей. Примерами могут служить атаки типа «отказ в обслуживании» (DoS-атаки), заключающиеся в перегрузке сети огромным количеством ложных запросов. Более сложный вариант – распределенные DoS-атаки (DDoS), когда атакующий трафик генерируется одновременно с большого числа компьютеров.

Нарушение аутентичности позволяет злоумышленнику выдавать себя за легального пользователя сети или сетевое устройство. Например, с помощью атаки «человек посередине» (Man in the Middle) злоумышленник может перехватывать и изменять трафик между пользователем и точкой доступа. Другая разновидность – создание ложной точки доступа для перехвата пользовательских данных.

Уязвимости беспроводных сетей связи обусловлены особенностями используемых протоколов и стандартов, несовершенством программного обеспечения, ошибками конфигурирования, человеческим фактором и др. Рассмотрим некоторые характерные примеры.

Протоколы аутентификации и шифрования данных, используемые в сетях WiFi стандарта 802.11, имеют ряд известных уязвимостей. Так, в протоколе WEP (Wired Equivalent Privacy) применяется слабый алгоритм RC4, который может быть взломан за считанные минуты. Протокол WPA (Wi-Fi Protected Access), хотя и усиливает защиту, но тоже подвержен атакам по словарю.

Особенность беспроводных сетей на базе протоколов IEEE 802.11 приводит к следующим сложностям защиты, по сравнению с проводными компьютерными сетями:

– для подключения к беспроводной сети не требуется физический доступ к кабелю витой пары или оптоволокну, достаточно находиться в зоне приема сигнала маршрутизатора;

– сама передача данных по беспроводному каналу может быть перехвачена и обработана даже без устройства доступа, специальными аппаратными или программными средствами[1].

К стандартным мерам защиты относятся программные и аппаратные средства, предназначенные для решения следующих задач:

– предотвращение несанкционированного подключения к беспроводной сети пользователей;

– предотвращение доступа к запрещенным ресурсам уже подключившихся пользователей.

Протоколы сотовой связи 2G (GSM) используют потоковые шифры A5/1 и A5/2 для шифрования передаваемых данных. Однако эти алгоритмы уже давно скомпрометированы – опубликованы эффективные методы их взлома. Несовершенна и процедура аутентификации абонентов с помощью алгоритма A3, допускающая клонирование SIM-карт.

В протоколах Bluetooth имеются уязвимости, позволяющие подбирать PIN-код для установления соединения методом полного перебора. Также возможны навязывание ложного адреса и перехват ключей шифрования на этапе установления соединения.

Протоколы беспроводных сенсорных сетей, такие как ZigBee, WirelessHART, допускают внедрение ложных пакетов, навязывание ложного маршрута, несанкционированное изменение конфигурации устройств из-за недостаточной защиты служебного трафика[2].

Таким образом, проведенный анализ показывает, что существующие протоколы беспроводной связи содержат уязвимости, которые могут использоваться злоумышленниками для реализации угроз информационной безопасности. Это обуславливает необходимость разработки новых методов оценки защищенности и обеспечения безопасности беспроводных сетей.

С развитием сетей связи нового поколения, таких как 5G и перспективные 6G, возникают новые вызовы в области информационной безопасности. Ожидается, что сети 6G будут обеспечивать сверхвысокие скорости передачи данных до 1 Тбит/с, минимальные задержки, а также связь не только на земле, но и в космосе, воздухе и под водой. Это открывает новые возможности для приложений виртуальной и дополненной реальности, Интернета Всего (Internet of Everything, IoE), где участниками сети будут не только устройства, но также процессы и данные.

---

[1] Богомолова Л.В. Информационная безопасность: что это такое в современных реалиях // Вестник науки и образования. 2023. № 1(132)-1. С. 45-48.

[2] Кушко Е.А. О вопросах безопасности передачи данных в сенсорной сети // Актуальные проблемы авиации и космонавтики. 2021. Т. 2. С. 384-386.

Вместе с тем открытая архитектура 6G, использование искусственного интеллекта для управления сетевыми операциями, а также подключение огромного числа IoT/IoE устройств с ограниченными ресурсами создают новые угрозы безопасности[1]. Традиционные меры защиты, такие как файерволы и VPN, могут оказаться недостаточными для сетей 6G из-за размытия границ между внутренней и внешней частью сети.

Одним из ключевых элементов архитектуры безопасности 6G должен стать принцип нулевого доверия (Zero Trust), предполагающий потенциальное наличие злоумышленника внутри сети. Для этого потребуется внедрение новых методов криптографии, устойчивых к атакам с использованием квантовых компьютеров (постквантовая криптография), улучшенная защита от новых типов атак, обновление протоколов аутентификации.

Важными требованиями к безопасности 6G являются:

– использование надежных систем виртуализации (гипервизоров, контейнеров) с возможностью обнаружения скрытых угроз;

– управление уязвимостями в компонентах с открытым кодом;

– обеспечение безопасности и конфиденциальности данных при использовании ИИ, например с помощью цифровых подписей моделей;

– сохранение конфиденциальности пользователей за счет хранения личных данных в доверенной среде и минимизации объема публично доступной информации.

В настоящее время запущен ряд международных проектов по исследованию и стандартизации технологий 6G, таких как Hexa-X, RISE-6G, NEW-6G. В рамках этих инициатив прорабатываются в том числе и вопросы безопасности сетей нового поколения.

Планируется использовать искусственные нейронные сети (ИНС) для прогнозирования времени до взлома беспроводных протоколов на основе их параметров. ИНС хорошо подходят для решения таких задач в условиях неполноты и неопределенности исходных данных.

Для обучения ИНС будет сформирован набор данных, содержащий информацию об основных параметрах распространенных протоколов беспроводной связи (WiFi, GSM, LTE и др.). В качестве входных параметров планируется использовать такие характеристики, как количество каналов, полоса частот, мощность, разнос каналов, наличие шифрования и др. Всего предполагается 11 входных параметров. Выходным параметром будет время до взлома протокола в годах, определенное на основе информации об обнаруженных уязвимостях и успешных атаках.

[1] Иброхимова Н.П. Современные методы и средства обеспечения информационной безопасности // Экономика и социум. 2024. № 8(123). С. 266-270.

Для поиска оптимальной структуры ИНС будет применяться методика, включающая перебор различных гиперпараметров – числа слоев и нейронов, типа функции активации, алгоритма оптимизации.

После обучения ИНС планируется использовать ее для прогнозирования времени до взлома новых перспективных протоколов, таких как NFC. Также будет проведен анализ значимости входных параметров, чтобы выявить характеристики протоколов, наиболее влияющие на их защищенность.

Таким образом, предлагаемый подход позволит прогнозировать устойчивость протоколов беспроводной связи к взлому на основе их параметров с помощью обученных ИНС. Это поможет заранее оценивать защищенность новых протоколов и выявлять ключевые характеристики, влияющие на безопасность.

Кроме технических мер защиты, большое значение имеет повышение осведомленности пользователей о правилах кибербезопасности. Операторам сетей 6G и сервис-провайдерам нужно будет регулярно информировать абонентов о потенциальных рисках и обучать методам противодействия, таким как использование сложных паролей, своевременное обновление ПО, осторожность при переходе по ссылкам и т.д.

В заключение можно сказать, что обеспечение безопасности сетей 6G станет одной из ключевых задач на пути к внедрению технологий связи нового поколения. Это комплексная проблема, требующая новых подходов и решений на разных уровнях – от разработки стандартов и архитектуры сети до внедрения продвинутых методов криптографии и искусственного интеллекта.

Минаев В.А.,

доктор технических наук, профессор
Московский университет МВД России им. В.Я. Кикотя

Кйеу Туан Ань, Нго Ван Нам, Нгуен Дык Дунг

Университет пожарной безопасности
Министерства общественной безопасности Вьетнама

Моделирование ресурсного обеспечения служб чрезвычайного реагирования (на примере противопожарной службы Вьетнама)

В статье рассматривается решение задач управления ресурсами служб оперативного реагирования на основе современных математических моделей. Базовыми выступают модели типологического анализа территорий и