Рисунок 1 – Схема работы прокси-сервера

VPN (Virtual Private Network) позволяет обеспечить одно или несколько сетевых соединений поверх другой сети, при этом используя средства криптографии (шифрование, аутентификация). Для реализации безопасной работы используются протоколы, где наиболее распространенным является PPTP. Он достаточно быстрый, легко настраиваемый, но при этом считается наименее защищенным по сравнению с другими. IPSec отвечает за шифрование и имеет более сильное шифрование, чем PPTP, устойчив к уязвимостям PPTP, обеспечивает также целостность сообщений и аутентификацию сторон. OpenVPN является безопасным, открытый и позволяет обходить многие блокировки, но требует отдельного программного клиента.

Рисунок 1 – Схема работы VPN

ЛИТЕРАТУРА

1. Threshold Proxy Re-Encryption Scheme and Decentralized Erasure Code in Cloud Storage With Secure Data Forwarding [Электронный ресурс]. – 2013. – Режим доступа: http://www.iosrjournals.org/iosr-jce/papers/Vol9-Issue5/E0952731.pdf?id=230

2. Кузнецов, А.А. Защита деловой информации (секреты безопасности). - М. Экзамен. 2008.

И.Б.БУРАЧЕНОК[1], В.К.ЖЕЛЕЗНЯК[1]

ВЫДЕЛЕНИЕ ИЗМЕРИТЕЛЬНЫХ СИГНАЛОВ ИЗ МАСКИРУЮЩИХ ШУМОВ ВЫСОКОГО УРОВНЯ В УСЛОВИЯХ ЗНАЧИТЕЛЬНОЙ НЕРАВНОМЕРНОСТИ АМПЛИТУДНО-ЧАСТОТНОЙ ХАРАКТЕРИСТИКИ

[1]*Учреждение образования «Полоцкий государственный университет», г. Новополоцк, Республика Беларусь*

В основе теории оценивания защищенности речевых сигналов (РС) в технических каналах утечки (КУ) основным критерием их защищенности, как правило, является коэффициент разборчивости речи (информационный показатель) – уровень разборчивости речи, воспринимаемый человеческим слухом за пределами выделенного помещения объекта информатизации (ОИ). Он равен нормативному численному значению словесной разборчивости речи [1]. В научной школе под руководством Покровского Н.Б. разработана формантная теория разборчивости русской речи с учетом ее статистических особенностей с использованием стандартных акустических таблиц ГОСТ Р 50840-95. Однако оценка разборчивости речи по инструментально-расчетному методу, предложенному Покровским Н. Б., весьма дорогостоящее и трудоемкое мероприятие (необходимо иметь целую артикуляционную экспертную бригаду). Поэтому чаще всего используется объективный метод оценки, когда разборчивость речи определяют по отношению мощности сигнала к мощности шума (ОСШ) (энергетический показатель), который математически зависим от разборчивости речи [2].

В Республике Беларусь оценка защищенности речевой информации (РИ) по техническим КУ на соответствие значениям, установленным нормативными требованиями к показателям эффективности защиты, регламентирована СТБ 34.101.29–2011. Оценка осуществляется при использовании гармонического измерительного сигнала (ИС) во всех технических КУ объектов информатизации, включая 1-ю категорию, в реальном масштабе времени с высокой точностью и высокой чувствительностью по численным значениям ОСШ и критерия разборчивости речи. Защищенность РС в техническом КУ оценивают выделением слабых ИС из шумов высокого уровня с учетом

неравномерности амплитудно-частотной характеристики (АЧХ), определяя ОСШ за пределами выделенного помещения ОИ при разбиении спектра РС (диапазон от 100 Гц до 10 кГц) на двадцать полос равной разборчивости (ПРР) с равными весовыми коэффициентами 0,05 [2].

В Руководстве по эксплуатации на «Комплекс переносной автоматизированный программно-аппаратный для измерения акустических и виброакустических параметров» «Филин А»» [3] установлено время излучения гармонических ИС в зависимости от влияющих факторов. Рекомендуемое время излучения гармонических ИС $T_{\text{с}}$=1, 10 и 25 с для каждой ПРР, что соответствует суммарному времени излучения всех ИС в двадцати ПРР, соответственно, $T_{\text{сум}}$=20, 200 и 500 с. Время излучения гармонического ИС определяется ослаблением преграды и степенью оценки защищенности РС по 1-й, 2-й и 3-й категориям. Для измерений с ослаблением преграды (например, стекольное ограждение, двери и т.п.) достаточно изучать гармонический ИС длительностью $T_{\text{с}}$=1 с, так как в точке приема за преградой его уровень достаточен для выделения на фоне шумов. Такой вид измерений используют для оценки защищенности РС по 3-й категории. Для преград с большим ослаблением преграды (например, кирпичные, железобетонные стены и т.п.) и необходимостью оценки защищенности РС по 1-й и 2-й категориям необходимо увеличивать время излучения гармонического ИС до $T_{\text{с}}$=10 с или $T_{\text{с}}$=25 с. Выделяемые оптимальным приемником полосы частот гармонических ИС с заданными длительностями равны: для сигналов длительностью $T_{\text{с}}$=1 с – 1Гц, $T_{\text{с}}$=10 с – 0,1Гц, $T_{\text{с}}$=25 с – 0,04Гц [2]. Таким образом, при ограничении времени излучения гармонического ИС его параметры ухудшаются, что приводит к снижению точности оценки в техническом КУ с явно выраженными неравномерностями АЧХ в измеряемом диапазоне частот. Методическая погрешность оценки защищенности РС гармоническим ИС помимо ограничения продолжительности сигнала не учитывает и ряд других факторов: линейные искажения входного сигнала и точность его передачи через систему звукопередачи; возможность предыскажений; ограничение полосы; значительные неравномерности АЧХ преграды (КУ речевой информации); его спектральную плотность в широком диапазоне частот и кривую чувствительности уха.

Для оценки защищенности речевой информации в техническом КУ с целью исключения методической погрешности, присущей гармоническому ИС предложено использовать сложный ИС с большой базой (значительно больше единицы). База сигнала B равна произведению длительности сигнала $T_{\text{с}}$ на ширину спектра частот $2\Delta f$ [4]. Предложенный для измерений сложный ИС имеет ряд особенностей и преимуществ перед гармоническим ИС: существенное сжатие при приеме с увеличением его амплитуды над уровнем помех; возможность одновременного повышения энергетического потенциала и разрешающей способности по частоте. Это позволило выделить из маскирующих шумов высокого уровня слабые ИС в условиях значительной неравномерности АЧХ.

Так как мощность шума определяется по формуле $P_{\text{ш}} = N_0 2\Delta f_k$, где $2\Delta f_k$ – ширина k-й ПРР, а N_0 – спектральная плотность мощности шума. Если энергия сигнала $E = P_{\text{с}} \cdot T_{\text{с}}$, где $P_{\text{с}}$ – мощность сигнала, равная $P_{\text{с}} = \frac{U_0^2}{R}$, ($R$=1 Ом), то ОСШ можно представить как $q^2 = \frac{2E}{N_0} = \frac{2P_{\text{с}}T_{\text{с}}}{P_{\text{ш}}} 2\Delta f_k$. Учитывая, что в широкополосных системах связи прием информации характеризуется ОСШ $h_0^2 = \frac{q^2}{2}$, экспериментально подтверждено преимущество при приеме сложного ИС на величину его базы, равную $B_k = 2\Delta f_k T_{\text{с}}$ в каждой отдельно взятой ПРР [4]. Доказанное преимущество предлагаемого для оценки сложного ИС с большой базой перед гармоническим ИС, равное величине базы сложного ИС, позволило при известной величине его базы установить величину разборчивости [4].

Обоснованные оптимальные значения базы сложного ИС в пределах ПРР спектра РС (в нашем случае при постоянном значении длительности $T_{\text{с}} = 4$ с в каждой отдельно взятой ПРР) позволили получить нормированные значения оценки защищенности речевой информации сложным измерительным сигналом.

Исследования процесса обнаружения слабых сложных ИС с большой базой с помощью процесса корреляции из шумов высокого уровня [5] показали, что в третьей полосе ПРР ИС сигнал обнаруживается при ОСШ –19±1 дБ, а в двадцатой полосе – при ОСШ –32±1 дБ. При формировании ИС при заданном уровне эффективной длительности сигнала $a = 1$ получены наилучшие результаты оценки [6].

ЛИТЕРАТУРА

1. Покровский, Н. Б. Расчет и измерение разборчивости речи / Н. Б. Покровский. – М. : Гос. Издательство литературы по вопросам связи и радио. 1962. – 392 с.

2. Железняк, В. К. Защита информации от утечки по техническим каналам: учеб. пособие / В. К. Железняк. – СПб. : ГУАП, 2006. – 188 с.

3. Бураченок, И. Б. Определение разборчивости речи в условиях воздействия шумов высокого уровня / И. Б. Бураченок, В. К. Железняк, К. Я. Раханов // Обеспечение пограничной безопасности и охрана Государственной границы Республики Беларусь : теория и практика : материалы 5-й науч.-практ. конф., Минск, 2015 г. / ГУО «ИПС РБ»; в 3 ч. редкол.: А. Е. Виноградов [и др.]. – Минск, 2015. – Ч. 1.– С. 228–231.

4. Железняк, В. К. Оценка нормативного показателя защищенности речевого сигнала сложным сигналом с большой базой / В. К. Железняк, И. Б. Бураченок // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2015. – № 12. – С. 10–14.

5. Бураченок И.Б., Железняк В.К., Раханов К.Я. Оценка разборчивости речи взаимной корреляцией сигнала линейной частотной модуляции в каналах утечки информации. // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2015. – №12. С. 22–27.

6. Бураченок, И. Б. Анализ измерительных сигналов для оценки защищенности речевой информации в технических каналах утечки / В. К. Железняк, И. Б. Бураченок // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2017. – № 4. – С. 2–8.

Ю.С.КУВЕЦКИЙ[1], И.Б.БУРАЧЕНОК[1]

ЗАЩИТА ИНФОРМАЦИИ ПЕРЕДАВАЕМОЙ ПО ПРОТОКОЛУ SOAP. БЕЗОПАСНОСТЬ WEB-СЕРВИСОВ (WS SECURITY)

[1]*Учреждение образования «Полоцкий государственный университет», г. Новополоцк, Республика Беларусь*

Во все времена необходимым условием развития человечества являлся процесс автоматизации различного вида его деятельности. Сегодня развитие передовых информационных технологий (ИТ) открывает новые возможности для создания современных автоматизированных систем (АС) во всех сферах народного хозяйства. Безусловно возникают и проблемы, связанные с необходимостью повышения уровня безопасности таких систем. Причем выбор методов и средств защиты определяется не только важностью обрабатываемой информации, но и составом АС, ее структурой, способами обработки информации, а также количественным и качественным составом пользователей и обслуживающего персонала. Рассмотрим систему, основными задачами которой являются удаленная компиляция и выполнение программного кода (ПК) на различных web-сервисах. Среди разработчиков современных программных приложений наиболее популярна сервисная архитектура – такие приложения гораздо проще поддерживать, легче решается задача масштабирования, но появляется проблема безопасности, т.к. происходит передача данных по сети. В данной статье мы рассмотрим вариант построения системы основываясь на протоколе передачи данных SOAP и стандарте обеспечения безопасности WS Security.

Во-первых, рассмотрим, что такое SOAP. Протокол SOAP (Simple Object Access Protocol) используется для обмена произвольными структурированными сообщениями в формате XML по распределенной вычислительной среде. Он может использоваться с любым протоколом прикладного уровня, однако чаще всего SOAP используется поверх HTTP (HyperText Transfer Protocol). Его сообщение в формате XML (eXtensible Markup Language) представляет из себя контейнер (envelope) содержащий заголовок (header) и тело (body), тело в свою очередь может содержать элемент с ошибками и статусом запроса (fault). Microsoft позволяет использовать протокол SOAP при помощи WCF (Windows Communication Foundation) [1].

Далее рассмотрим три стандарта безопасности применимых к XML: аутентификация, целостность данных, конфиденциальность данных.

Аутентификация гарантирует, что отправитель и получатель являются теми, кем они себя объявляют, доказывает подлинность сторон. Это может реализовываться различными способами. Простой вариант – предоставить идентификатор пользователя и его пароль. Более сложный – это