современных звукозаписывающих и звуковоспроизводящих устройств позволяет злоумышленнику фальсифицировать в процедурах аутентификации биометрический образ зарегистрированного в системе пользователя [2].

Развитием идентификации личности по голосу является контактно-разностный метод, использующий акустические характеристики человеческого тела в качестве биометрического параметра для идентификации. При этом акустическую модель тела человека можно представить в виде сложной уникальной системы проводников звукового сигнала, формируемого в носоглотке человека при произнесении каких-либо звуков. Использование специальных датчиков ларингофонного типа позволяет регистрировать звуковые сигналы, распространяющиеся через биологические жидкости, мягкие и твердые ткани человека, с последующим формированием индивидуального биометрического образа. При идентификации сигналы снимаются с выбранной области регистрации колебаний — это может быть, например, голова, плечо, локоть, запястье руки, колено и т. п. Следует отметить, что для различных точек наблюдения (областей регистрации) сигнала, вследствие разных трактов звукопередачи, акустические характеристики принимаемых колебаний будут отличаться. Таким образом, если злоумышленник не знает область регистрации акустического сигнала, то фальсификация такого принимаемого колебания существенно усложняется [2].

СПИСОК ЛИТЕРАТУРЫ:

1. *Голубинский А. Н., Булгаков О. М.* Система аутентификации личности по голосу на основе математической модели речевого сигнала // XXIII Международная научная конференция «Математические методы в технике и технологиях»: Сборник трудов. Т. 6. Саратов, 2010. С. 19–22.
2. *Голубинский А. Н., Дворянкин С. В.* Обработка акустических сигналов при контактно-разностном методе идентификации личности // Безопасность информационных технологий. 2011. № 3. С. 10–16.

Д. С. Чернявский

УНИФИКАЦИЯ ПРАВИЛ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ СРЕДСТВ ЗАЩИТЫ

Для повышения эффективности разработки и реализации политики информационной безопасности (ИБ) необходимо унифицировать способ задания правил политики и процесс настройки сетевых средств защиты (ССЗ) [1]. Предлагаемым решением является унифицированный язык правил политики ИБ ССЗ [2] (далее — унифицированный язык), который позволяет задавать и реализовывать правила политики ИБ независимо от пользовательских интерфейсов и внутреннего устройства конкретных ССЗ.

В общем случае правило политики ИБ, формализованное с использованием унифицированного языка, имеет следующий синтаксис:

Identifier action function1(param11 ... param1N) ... functionK(paramK1 ... paramKM),

здесь *identifier* — некоторый идентификатор правила, *action* — действие, *Function1 … functionK* $(K \in^{N})$ — функции безопасности, выполняемые ССЗ, с параметрами *param11 … param1N*, *paramK1 … paramKM* $(N,M \in^{N_0})$. Порядок и структура параметров зависят от конкретной функции. На данный момент унифицированный язык поддерживает формализацию функций

фильтрации сетевого трафика, маршрутизации, трансляции адресов, формирования сообщений безопасности, а также позволяет комментировать правила.

Например, правила фильтрации сетевого трафика на унифицированном языке используют функции анализа сетевого трафика канального, сетевого и транспортного уровней и любое из данных правил имеет следующий синтаксис:

Identifier action function1(param11... param1N) function2(param21... param2K) function3(param31...param3M) function4(param41...param4L),

здесь *Function1* — ключевое слово, обозначающее одну из функций анализа трафика канального уровня, к которым в данной спецификации языка относится функция анализа заголовка Ethernet-кадра; *Function2* — ключевое слово, обозначающее одну из функций анализа трафика сетевого уровня, к которым в текущей спецификации языка относится функции анализа IPv4-заголовка; *Function3* — ключевое слово, обозначающее одну из функций анализа трафика транспортного уровня, к которым в данной спецификации языка относится функции анализа TCP-заголовка, UDP-заголовка и ICMP-заголовка.

Пусть сетевая политика ИБ содержит следующее требование: «*Доступ к серверу* 10.1.1.10 *может осуществляться только из сети* 192.168.1.0/24 *и только по протоколу http. Все обращения к серверу должны записываться в лог-файл*». На унифицированном языке рассматриваемое правило задается так:

permit log IP(192.168.1.0/24 10.1.1.0) TCP (80*)*

или в более компактной форме:

*log IP 192.168.1.0/24 10.1.1.0 TCP * 80.*

Для того чтобы реализовать правило в конфигурации ССЭ, используется транслятор унифицированного языка, который производит синтаксический анализ правила на унифицированном языке, устанавливает соединение с ССЭ и производит его настройку.

В основу синтаксиса и семантики унифицированного языка положены функциональные возможности ССЭ. Опираясь на функции безопасности, язык может быть использован для описания политик ИБ для заранее не определенного класса ССЭ. Функции, являющиеся основой синтаксической структуры языка, с семантической точки зрения эквивалентны понятию функции безопасности модели ГОСТ ИСО/МЭК 15408 [3], т. е. функциональным возможностям части или частей системы, обеспечивающим выполнение подмножества взаимосвязанных правил политики ИБ организации. В то же время правила политики ИБ, формализованные с использованием данного языка, с точки зрения семантики являются политикой функции безопасности — политикой ИБ, осуществляемой функцией безопасности.

Грамматика унифицированного языка построена таким образом, что в нее могут быть легко добавлены новые функции безопасности, а следовательно, и поддержка новых типов правил политики ИБ. При этом такое расширение грамматики не повлияет на общую логику построения правил политики ИБ с использованием языка. Данное свойство языка обеспечивает выполнение требования расширяемости языка. Грамматика унифицированного языка является контекстно-свободной, что делает язык относительно простым не только с точки зрения построения предложений, но и с точки зрения его синтаксического анализа и последующего использования предложений языка.

Унифицированный язык удовлетворяет следующим требованиям [4]:

— *Наглядность и простота*. Правила политики ИБ, формализованные с помощью языка, должны быть простыми для понимания и исключать возможность некорректной трактовки. Выполнение данного требования позволяет снизить вероятность обхода правила в случае его сложности или его неправильной реализации в случае неверного понимания;

— *Отсутствие абстрактных понятий в структуре языка*. Правила политики ИБ, формализованные с помощью языка, должны состоять из структурных элементов, описание

которых должно быть однозначно сопоставимо с реальными объектами, действиями и процессами. Выполнение данного требования позволяет избежать возможности неоднозначной трактовки правил политики ИБ;

— *Поддержка широкого спектра правил политики ИБ*. Чем шире этот спектр, тем более универсальным является язык;

— *Применимость к конкретным системам*. Правила политики ИБ, формализованные с помощью языка, должны быть транслируемы в форматы данных и языки конкретных систем. Выполнение этого требования позволяет решить проблему реализации политики ИБ в качестве конфигурации различных систем безопасности;

— *Расширяемость*. Язык должен быть формализован таким образом, чтобы при добавлении нового типа правил ИБ в спецификацию языка общая структура предложений языка оставалась неизменной. Выполнение данного требования позволяет сделать язык применимым к большему числу типов политик и систем путем его расширения;

— *Открытость спецификации*. Выполнение данного требования обеспечивает возможность расширения языка и его применения к конкретным системам не только разработчиком языка, но и другими заинтересованными сторонами.

СПИСОК ЛИТЕРАТУРЫ:

1. *Thayer R.* Network Security: Locking in to Policy // Data Communications. 1988. № 4.
2. *Chernyavskiy D., Miloslavskaya N.* Unified Language for Network Security Policy Implementation // Proceedings of ICNS 2011: The Seventh International Conference on Networking and Services. 2011.
3. ГОСТ ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
4. *Dongliang J., Lianzhong L., Shilong M., Xiaoni W.* Research on Security Policy and Framework // Proceedings of the Second International Symposium on Networking and Network Security (ISNNS10). 2010.

В. Б. Щербаков

МЕТОДИКА РИСК-АНАЛИЗА ПРОЦЕССА ПЕРЕХВАТА РАДИОСИГНАЛОВ БЕСПРОВОДНОЙ СЕТИ

Существуют различные подходы к определению мер риска, существенно зависящие от методики оценки их значений. Исходя из этих мер могут быть получены некоторые прогнозные оценки.

Для риск-анализа процесса перехвата радиосигналов беспроводной сети предлагается методический подход, основанный на следующих показателях: гипотеза H_0 соответствует отсутствию сигнала на входе приемника; гипотеза H_1 — наличию сигнала; γ_0 — решение принять гипотезу H_0; γ_1 — решение принять гипотезу H_1. Ущерб предлагается оценивать величиной $\frac{Y_{ñø}}{N_0}$, где $Y_{ñø}$ — накопленная энергия смеси сигнала и шума, а N_0 — спектральная плотность мощности шума.

Тогда введем понятие матрицы ущербов:

$$C = \begin{pmatrix} C_{00} & C_{01} \\ C_{10} & C_{11} \end{pmatrix}, C_{01} > C_{00} \geq 0, C_{10} > C_{11} \geq 0, \quad (1)$$