4. ***Широчин, В. П.*** Динамическая аутентификация на основе анализа клавиатурного почерка / В. П. Широчин, А. В. Кулик, В. В. Марченко. – Режим доступа: http://www.masters.donntu.edu.ua, свободный. – Заглавие с экрана. – Яз. рус.

УДК 004.056.55

ВЫБОР СРЕДСТВ ЗАЩИТЫ ДЛЯ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА

Р.Ю. Волик

Рассматриваются вопросы выбора средств защиты информации при построении виртуальных частных сетей (VPN) с целью организации систем защищенного информационного взаимодействия между распределенными сетями и вопросы обеспечения безопасности при передаче информации с использованием сетей общего доступа.

Ключевые слова: *виртуальная частная сеть, межсетевые экраны.*

Key words: *virtual private network, firewall.*

В настоящее время широкое распространение получает электронный документооборот как один из видов электронного взаимодействия между сторонами в виде информационного обмена.

Информационные системы становятся сегодня одним из главных инструментов управления бизнесом, важнейшим средством производства современного предприятия.

Одновременно с внедрением средств обеспечения электронного документооборота и, как следствие, повышением производительности предприятия возникает вероятность реализации угроз информационной безопасности, которым могут быть подвержены информационные ресурсы предприятия. Поэтому вопрос обеспечения безопасности информации при осуществлении документооборота встает наиболее остро.

Защита информации в процессе ее передачи по открытым каналам основана на построении защищенных виртуальных частных каналов связи, называемых туннелями VPN. Туннель VPN обладает свойствами защищенной выделенной линии, причем эта защищенная выделенная линия развертывается в рамках общедоступной сети, например интернет-сети. Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты виртуальной сети.

VPN создает виртуальные защищенные «туннели» в открытых TCP/IP сетях типа интернет-сети. Наличие «туннеля» позволяет решить двойную задачу:

- исключить перехват проходящей по «туннелю» информации;
- исключить подключение незарегистрированного компьютера к VPN, изменение информации и любые сетевые атаки.

VPN-продукты позволяют организовывать защищенные туннели между офисами компании. При этом абсолютно неважно, через какого провайдера конкретная рабочая станция подключится к защищенным ресурсам предприятия. По оценке CNews, относительная доля VPN на российском рынке ИБ уже достигает 30 % [3, 4].

VPN технология обеспечивает:

- защиту (конфиденциальность, подлинность и целостность) передаваемой по сетям информации;
- контроль доступа в защищаемый сектор сети;
- безопасный доступ пользователей VPN к ресурсам сетей общего пользования;
- централизованное управление политикой корпоративной сетевой безопасности.

Использование сетей общего пользования в качестве транспортной сети возможно при выполнении определенных требований.

1. Организация безопасного доступа и разграничение доступа к сегментам с использованием межсетевых экранов, сертифицированных по требованиям ФСБ, ФСТЭК.

2. Организация VPN с применением сертифицированных требований ФСБ России, ФСТЭК криптографических СЗИ для обеспечения передачи данных через сеть общего пользования между закрытыми сегментами при межобъектовом взаимодействии.

Рынок VPN развивается сегодня весьма бурно, предлагая компаниям широкий выбор оборудования и программного обеспечения для этих сетей – от интегрированных многофункциональных и специализированных устройств до чисто программных продуктов.

Предварительный анализ российского и зарубежного рынка программно-аппаратных средств защиты показал, что спектр таких продуктов чрезвычайно широк и в тоже время отсутствует единая методика выбора средств защиты.

В результате анализа методик выбора средств защиты наиболее рациональной является методика, предложенная А. Лукацким [1, 2]. Метод основан на последовательном прохождении ряда шагов, ведущих к оптимальному результату.

Этап 1. Определим критерии выбора средств защиты. Критерии сравнения функциональности средств сетевой защиты – наиболее неоднозначная область. Вопрос о том, по каким критериям сравнивать VPN-продукты, как же все-таки выбрать именно то, что надо, сегодня задают себе многие. А вот однозначно на него ответить не так просто. Основная трудность, с которой приходится сталкиваться при сравнении функциональности VPN-решений различных производителей, очень тонкая грань между тривиальными и существенными критериями. Анализ литературы показал, что для оценки VPN используются различные критерии. Рассмотрим эти критерии подробно.

Контроль доступа – первый критерий выбора будущего средства защиты. Он позволит отслеживать доступ пользователей к внешним Интернет-ресурсам.

Следующий критерий – это производительность системы, VPN-устройство, интегрированное в корпоративную сеть, не должно влиять на ее производительность. Узким местом в данной задаче становится шифрование данных – именно этот процесс вносит основной вклад в снижение пропускной способности VPN-тоннеля. К тому же в процессе туннелирования данных к ним неизбежно добавляется служебная информация, что тоже отнимает на себя часть полосы пропускания. В этой связи актуальным становится наличие встроенной возможности сжатия данных.

Продукт должен быть прост в установке и настройке, не требовать изменения топологии сети, изменения сложившейся политики взаимодействия с внешней сетью общего пользования.

Немаловажные критерии – простота эксплуатации, необходимость обучения персонала.

Необходимым условием, предъявляемым к продукту, будет способность работать в автономном режиме, не требующем присутствия и вмешательства администратора при нормальной работе.

Следующий критерий – возможность удаленно и централизованно управлять всеми компонентами VPN. Этот критерий способствует и более строгому соблюдению корпоративной политики безопасности, поскольку сотрудники на местах могут быть лишены возможности переконфигурировать располагающиеся у них VPN-устройства.

Следующий критерий – возможность «холодного» и «горячего» резервирования – позволит восстановить работоспособность сегмента сразу после ремонта или замены вышедшего из строя оборудования.

Возможность масштабирования продукта – один из немаловажных критериев. Подключение дополнительных сегментов не должно требовать переконфигурации имеющихся.

Такой критерий, как число поддерживаемых сетевых интерфейсов, позволит сразу оценить гибкость приобретаемого решения: возможно ли будет одним VPN-модулем обеспе-

чить защиту нескольких сегментов корпоративной сети. Некоторые VPN-продукты предоставляют возможность разделять доступ между внутренними сегментами сети, что позволяет максимально адаптировать продукт к принятой корпоративной политике безопасности.

Кроме того, для каждого продукта в системе защиты должна существовать своя «инфраструктура», включающая комплект документации (желательно на русском языке), наличие у поставщика авторизованного обучения, квалифицированных консультаций и т.д. Все эти аспекты также должны приниматься во внимание при выборе того или иного продукта.

При формулировании критериев к выбору средств защиты необходимо учитывать наличие сертификата соответствия требованиям регулирующих органов.

Этап 2. Присвоим каждому выбранному критерию весовой коэффициент, указывающий на степень его важности (см. табл. 1). Сумма весовых коэффициентов должна равняться единице.

Таблица 1

Оценка критериев выбора средств защиты

Критерии выбора средств защиты	Весовой коэффициент
1. Критерий 1	P_1=
2. ...	…
3. Критерий N	P_N=

Этап 3. Проанализируем наличие и качество реализации необходимых функций в подмножестве средств защиты (см. табл. 2).

Таблица 2

Определение качества реализации функции средств защиты

Функция		Качество реализации функции
Критерий 1	Средство защиты 1	К=
	Средство защиты 2	К=
	Средство защиты 3	К=
…		
Критерий N	Средство защиты 1	К=
	Средство защиты 2	К=
	Средство защиты 3	К=

Этап 4. Для каждой участвующей в выборе системы защиты умножаем вес показателя на выставленный балл, после чего суммируем полученные значения.

$$R_{1..n} = K_{1..n} \cdot P_{1..n} \quad (1)$$

$$R_{\text{ПРОДУКТ}} = \sum_{1}^{n} R \quad (2)$$

где $P_{1..n}$ – весовой коэффициент;

$K_{1..n}$ – качество реализации функции;

R_{max} – наилучший продукт.

Из полученного набора итоговых оценок необходимо выбрать максимальную. Набравшее её средство защиты и является наилучшим.

Таким образом, при выборе средств защиты для построения системы защищенного информационного обмена необходимо, в первую очередь, определить критерии, по которым будут оцениваться средства защиты. Крайне важно помнить, что эффективность этого метода зависит от верного подбора оцениваемых показателей и выставления им правильных весовых коэффициентов. Если будет допущена ошибка на первом и втором шагах, то вся последующая работа пойдет по ложному пути и приобретенное в итоге средство не будет отвечать необходимым требованиям.

Библиографический список:

1. ***Лукацкий, А. В.*** Системы обнаружения атак / А. В. Лукацкий // Банковские технологии. – 1999. – № 2.

2. ***Лукацкий, А. В.*** Средства анализа защищенности – сделайте правильный выбор / А.В. Лукацкий // PCWEEK. – 2003. – № 46.

3. ***Панасенко, Е.*** Российский рынок ИБ растет быстрее ИТ / Е. Панасенко. – Режим доступа: http://www.cnews.ru, свободный. – Заглавие с экрана. – Яз. рус.

4. ***Соколова, А. А.*** Оценка экономической эффективности внедрения VPN-решений / А. А. Соколова, И. А. Филиппова // Information Security / Информационная безопасность. – 2007. – № 1. – С. 44–45.

УДК 681.3.067

МЕТОДЫ ИДЕНТИФИКАЦИЯ ЗВУКОВЫХ ПЛАТ ПО СОЗДАВАЕМЫМ ЗВУКОВЫМ ДАННЫМ*

В.М. Федоров, О.Б. Макаревич, Д.П. Рублев, А.Б. Чумаченко

Рассматриваются методы идентификации звуковых плат по создаваемым ими звуковым файлам на основе неоднородностей, вносимых аппаратной частью плат. Рассмотрены два метода идентификации: с использованием гауссовских смешанных моделей и нейронных сетей. Показана работоспособность обоих методов, однако точность идентификации с использованием нейронных сетей выше, чем при использовании метода гауссовских смешанных моделей.

Ключевые слова: *идентификация цифровых устройств записи, спектрограмма, коэффициенты линейного предсказания, кепстр, нейронные сети, гауссовские смешанные модели.*

Key words: *digital recording devices identification, spectrogram, linear prediction coefficients, cepstrum, artificial neural networks, Gaussian mixed models.*

За последние десятилетия вместе с массовым вытеснением аналоговых средств звуко- и видеозаписывающей техники компактными цифровыми устройствами стала актуальной задача их идентификации, а также подтверждения подлинности получаемых с их помощью образов. Как известно, аналоговые и цифровые образы, полученные при помощи любого устройства записи, несут в себе набор особенностей, сформированных различными узлами тракта записи, что позволяет (при наличии предполагаемого устройства записи) во многих случаях однозначно установить принадлежность ему образа.

В данной работе рассматривается возможность идентификации звуковых карт, подключаемых при помощи USB-интерфейса, а также звуковых карт на основе кодека AC'97, встроенных в материнскую плату ПЭВМ. При записи в записанных файлах создаются устойчивые особенности, характерные исключительно для данных звуковых плат. Таким образом, признаки аппаратной части – это устойчивые во времени отклонения характеристик сенсора и последующих блоков обработки, включая АЦП как отдельного устройства. Для устройств аудиозаписи к таковым относятся отклонения от средней АЧХ, внутренние наводки на аналоговую часть, отклонения характеристик АЦП, нестабильность генераторов тактовой частоты и т.д. Упрощённая схема обработки сигнала в цифровой звуковой карте приведена на рис.

* Работа выполнена при поддержке грантов РФФИ 08-07-00253-а и 09-07-00242-а.