Усков А.В., Иванников А.Д., Усков В.Л.

ОБОБЩЕННАЯ МЕТОДИКА ПОСТРОЕНИЯ VPN-РЕШЕНИЙ ДЛЯ СИСТЕМ ИНФОРМАЦИОННОЙ ЗАЩИТЫ КОРПОРАТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ СЕТЕЙ

uskov@insightbb.com
Государственный НИИ информационных технологий и телекоммуникаций
г. Москва

Вступление

Технология виртуальных частных защищенных сетей Virtual Private Networks (VPN) – VPN-технология - стремительно развивается в последние годы [1,2,3]. Крупнейшие организации во всем мире – государственные структуры, крупные корпорации, учреждения, банки, крупные образовательные организации - планируют массовое использование VPN-технологии в ближайшем будущем. Связано это с тем, что информационная безопасность (ИБ) в корпоративных сетях, использующих VPN-технологию, может достигать очень высокой эффективности и удовлетворять основным принципам безопасной передачи и обработки данных в компьютерных сетях [3]:

1. принципу аутентификации, т.е. установления подлинности взаимодействующих сторон (объектов сети, пользователей сети), обеспечения безопасного входа в сеть легитимных пользователей и предотвращения доступа к сети нежелательных пользователей и устройств;
2. принципу конфиденциальности, т.е. защите передаваемой информации от несанкционированного чтения и копирования; этот процесс может осуществляться на основе различных криптографических алгоритмов шифрования;
3. принципу целостности (интегрированности), т.е. обеспечения неизменности и сохранности передаваемых данных;
4. принципу управления доступом и авторизации, т.е. обеспечения правом пользования сетевыми ресурсами и сервисами исключительно тех объектов и пользователей сети, которые доказали свою аутентичность (легитимность);
5. принципу защиты анализа сетевого траффика, т.е. сокрытия происходящего процесса обмена информацией в туннеле и идентификации (определении) участвующих в этом процессе объектов или пользователей сети от любого человека или устройства, анализирующего трафик (активность) сети;
6. принципу исключения дублирования пакетов данных, т.е. обеспечения использования одних и тех же пакетов данных только один раз.

Обеспечение ИБ на уровне деятельности компьютерных сетей организации определяется нормативно-правовыми основами и доктриной ИБ РФ. Но

построение стратегий ИБ и практических решений по ее реализации зависит от самой организации. *Стратегия ИБ (СИБ)* – это множество требований, политик, технологий и процедур ИБ, используемых в организации. Современной парадигмой разработки СИБ является *формальное описание* СИБ, основанное на использовании моделей систем защиты информации (СЗИ). *Модель СЗИ* – это абстрактное описание поведения целого класса СЗИ без рассмотрения конкретных деталей их практической реализации.

Под *открытой* (публичной) внешней средой передачи информации ниже понимается всемирная компьютерная сеть Интернет; под *объектами* корпоративной образовательной сети (КОС) - коммуникационные модули, серверы и компьютеры (хосты), программно-аппаратные средства (концентраторы, маршрутизаторы, межсетевые экраны, шлюзы (мосты), и т.п.), работающие по сетевым технологиям открытой внешней среды. Под термином *виртуальная защищенная сеть VPN* (сетью VPN) КОС ниже понимается объединение объектов КОС в единую виртуальную сетевую структуру через открытую внешнюю среду передачи информации. Сети VPN формируются путем построения виртуальных защищенных каналов связи, называемых туннелями VPN. Термином *туннель VPN* будем называть соединение различных объектов КОС, которое скрытно «проложено» в открытой внешней сети и по которому передаются криптографически защищенные пакеты данных.

Ниже рассматриваются вопросы разработки базовой модели ИБ для класса СЗИ КОС на основе взаимодействия объектов открытой внешней сети и туннелей VPN (СЗИ-VPN), а также обобщенной методики построения практических решений для СЗИ-VPN (VPN-решений), основанной на разработанной базовой модели.

Базовая модель СЗИ-VPN КОС

Предлагаемая базовая модель определяет общие принципы построения системы СЗИ-VPN КОС. Ее основными элементами являются:

O – множество объектов в КОС,
S – множество субъектов (пользователей) в КОС, причем пользователями в данном случае могут выступать как люди (подмножество *U*), так и разнообразные программные приложения (подмножество *SWA*),
R – множество видов прав доступа субъектов *S* к объектам *O*, например, права на чтение (*read*) данных, их копирование (*copy*), модификацию (*modify*) и др.,
AP – множество архитектурных решений построения сетей VPN,
TP – множество технических решений реализации сетей VPN,
CP – множество схемных решений при построении сетей VPN,
УР - множество уровней модели взаимодействия открытых систем OSI, используемых в сети VPN, или множество уровневых решений (УР),
P – множество протоколов защиты информации, используемых в сетях VPN,
AA – множество алгоритмов аутентификации участвующих сторон,
AC – множество используемых криптографических алгоритмов шифрования,

АК – множество алгоритмов управления ключами и согласования параметров протоколов, используемых в сети VPN,
MOD - множество режимов использования протоколов сетей VPN,
PAR - множество параметров протоколов, технологий, алгоритмов и методов используемых в сетях VPN,
t = 0, 1, 2, … – время,
$St \subset Ot$ – множество субъектов КОС в момент времени *t*,
$Gt = (Ot, Et)$ - граф текущих доступов в КОС в момент времени *t*, где *Ot* – вершины графа, $Et \subset Ot \times Ot \times R$ – множество ребер (каждое ребро соответствует текущему доступу в КОС в момент времени *t*),
Go – граф текущих доступов в начальном состоянии КОС,
Gp – множество всех последовательностей графов текущих доступов в КОС (каждая последовательность соответствует заданной траектории функционирования сети).

На основании основной аксиомы теории защиты информации («Все вопросы безопасности информации описываются доступами субъектов к объектам») [4] можно утверждать, что, в общем случае, свойства СЗИ КОС могут быть определены на основании описания свойств графов последовательностей из *Gp*. Среди всех возможных последовательностей из *Gp*, согласно требованиям разработанной СИБ КОС и отдельных политик ИБ, априорно выделяются два подмножества последовательностей: 1) *Gl* – подмножество легитимных (разрешенных, допустимых) траекторий, 2) *Gn* – подмножество нелегитимных (запрещенных, неразрешенных) траекторий ($Gp = Gl \cup Gn$, $Gl \cap Gn = \varnothing$).

Стратегия ИБ КОС состоит в том, чтобы любая реальная траектория *Gr* функционирования КОС не попала в множество нелегитимных траекторий *Gn* в пространстве безопасности КОС, которое, в самом общем случае, будет выглядеть как декартово произведение: $O \times S \times R \times AP \times CP \times TP \times УР \times P \times AA \times AC \times AK \times MOD \times PAR$.

Элементы базовой модели СЗИ-VPN КОС

Рассмотрим базовые элементы множеств АР, СР, ТР, УР, Р, АА, АС, АК, MOD, PAR.

Множество архитектурных решений *AP* описывает возможные архитектуры построения сети VPN и включает в себя следующие элементы: 1 – архитектуру типа «внутрикорпоративная сеть VPN» (АР=1), 2 – архитектуру типа «межкорпоративная сеть VPN» (АР=2), 3 – архитектуру типа «сеть VPN с удаленным доступом» (АР=3), 4 – интегрированную архитектуру, которая может объединять различные архитектурные элементы вышеуказанных решений.

Множество схемных решений *CP* описывает возможные схемы построения сетей VPN и включает в себя следующие элементы: 1 – схема типа «хост-N – хост-M» (СР=1), 2 – схема типа «шлюз-N – шлюз-M» (СР=2), 3 – схема типа «хост-N – шлюз-V» или «шлюз-N – хост-M» (СР=3), 4 – интегрированное решение, которое может объединять несколько вышеуказанных схем-

ных решений. Отметим, что параметром элементов множества является тип используемой операционной системы (1=Windows, 2=UNIX/Linux, 3=Mac); таким образом, указание «хост-1 – шлюз-2» говорит о том, что на одном конце VPN-туннеля хост (пользовательский компьютер) работает под операционной системой Windows, а на другом конце VPM- туннеля - шлюз сети работает под операционной системой UNIX/Linux.

Множество технических решений *TP* описывает возможные способы технического построения сети VPN и во многом определяет ее технические спецификации и характеристики; это множество включает в себя следующие элементы: 1 – сеть VPN на основе программного обеспечения, 2 – сеть VPN на основе маршрутизаторов, 3 – сеть VPN на основе межсетевых экранов или брандмауэров, 4 – сеть VPN на основе специализированных программно-аппаратных устройств, 5 – интегрированное решение, которое может объединять несколько вышеуказанных частных технических решений.

Множество уровней модели взаимодействия открытых систем OSI, используемых в сети VPN, или множество уровневых решений *УР* описывает используемый системой СЗИ-VPN «рабочий» уровень из модели OSI [1], а также содержит информацию о протоколах, направленных на защиту передаваемых данных; это множество включает в себя следующие элементы: 2 – сеть VPN канального уровня (УР=2), 3 – сеть VPN сетевого уровня (УР=3), 5 – сеть VPN сеансового уровня (УР=5).

Множество протоколов *P*, ориентированных на защиту информации в сетях VPN, включает в себя следующие элементы: 1 - протокол передачи данных второго (канального) уровня L2F; 2 - протокол туннелирования данных второго (канального) уровня L2TP; 3 - протокол туннелирования для двухточечного соединения PPTP; 4 - стек протоколов безопасного межсетевого обмена IPSec, который включает в себя протоколы IKE, AH, ESP; 5 - протокол согласования параметров виртуального канала и управления ключами в сети Интернет IKE; 6 - протокол аутентифицирующего заголовка AH; 7 - протокол инкапсулирующей защиты содержимого ESP; 8 - протокол защищенных сокетов SSL; 9 - протокол защиты транспортного уровня TLS; 10 - протокол обеспечения приложений типа клиент-сервер сервисами, расположенными за межсетевыми экранами SOCKS; 11 – протокол обеспечения удаленного управления операционной системой и передачи файлов SSH; 12 – система удаленной аутентификации пользователей по коммутируемым линиям RADIUS; 13 – протокол централизованного контроля удаленного доступа TACACS; 14 – протокол аутентификации на основе процедуры «запрос-ответ» CHAP; 15 - протокол аутентификации по паролю PAP.

Отметим, что множество *P* разработанной общей модели СЗИ-VPN включает только избранные протоколы защиты информации, которые, по мнению авторов, продемонстрировали высокую эффективность и надежность защиты информации при работе в различных компьютерных системах; некоторые дополнительные протоколы описаны в [7].

Множество алгоритмов аутентификации *AA* включает в себя следующие базовые элементы: 1 - аутентификация на основе технологии *цифровой*

подписи; 2 - аутентификация на основе технологии *цифровых сертификатов стандарта X.509*; 3 - аутентификация на основе технологии *активной директории (серверов системы Kerberos)*; 4 - аутентификация на основе технологии *разделяемого секрета.*

Множество криптографических алгоритмов *AC* *{AC} = {{AC-S}, {AC-P}, {AC-D}, {AC-H}, {AC-X}}* включает в себя подмножества и элементы, представленные в Табл. 1.

Таблица 1.

Криптографические алгоритмы для использования в СЗИ-VPN

Подмножество	Некоторые популярные криптографические алгоритмы [5] - элементы подмножества
{AC-S} блочные симметричные алгоритмы шифрования с закрытым ключом	1 - алгоритмы на базе стандарта ГОСТ 28147-89
	2 - алгоритмы на базе стандарта шифрования AES
	3 – алгоритмы на базе стандарта DES
	4 - алгоритм IDEA
	5 - семейство алгоритмов RCA (RCA2, RCA4)
{AC-P} асимметричные алгоритмы шифрования с открытым ключом	6 - алгоритм Эль-Гамаля 7 - алгоритмы RSA
{AC-D} алгоритмы цифровой подписи	8 - алгоритмы на базе ГОСТ Р 34.10-2001
	9 - алгоритмы DSA
{AC-H} алгоритмы на базе функций хэширования	10 - алгоритм SHA-1 11 - алгоритм MD5 12 - алгоритм HMAC
{AC-X} алгоритмы распределения ключей	13 - алгоритм Диффи-Хеллмана

Отметим, что множество *AC* разработанной общей модели СЗИ-VPN включает только избранные криптографические алгоритмы, которые, по мнению авторов, продемонстрировали высокую эффективность и надежность защиты информации при работе в различных компьютерных системах. Некоторые дополнительные криптографические алгоритмы описаны в [5,7].

Множество алгоритмов управления ключами и согласования параметров протоколов *АК*. Данное множество описывается как *{AK} = {{AC-S}, {AC-P}, {AC-X}}* и включает в себя подмножества и элементы, представленные в Табл. 1.

Множество режимов *MOD* по использованию протоколов *P* сетей VPN описывает возможные режимы использования протоколов защиты информации в сети VPN и включает в себя следующие элементы: 1 – туннельный режим (MOD=1), 2 – транспортный режим (MOD=2).

Множество параметров *PAR* протоколов *P* и алгоритмов *AA* и *AC*, используемых в СЗИ-VPN, описывает многочисленные параметры настройки, управления и функционирования протоколов, технологий, алгоритмов и методов, используемых при практическомм построении СЗИ-VPN и влияющих на

эффективность системы защиты. Ввиду большого количества элементов данного множества (более 150) и в связи с ограничением на объем публикации детальное описание параметров опущено.

Описанные выше множества *AP, TP, CP, УР, P, AA, AC, AK, AC-S, AC-P, AC-D, AC-H, AC-X, MOD, PAR* являются конечными и расширяемыми множествами в базовой модели СЗИ-VPN. В связи с этим, множество траекторий *M,* создаваемых на основе обобщенной модели СЗИ-VPN, является также конечным и расширяемым множеством.

Обобщенная методика построения решений СЗИ-VPN КОС

СЗИ КОС, является, во-первых, частью КОС, а во-вторых, программно-аппаратной системой, имеющей конечные технические ресурсы (производительность, память, и др.). Следовательно, в общем случае, для полноценного решения задачи защиты информации в КОС ее СЗИ, обладающая конечными ресурсами, должна в каждый момент времени хранить и анализировать информацию обо всей предыстории функционирования КОС, а также предсказывать будущее КОС, что является алгоритмически неразрешимой задачей.

Таким образом, задача построения абсолютно (100%) надежной СЗИ КОС должна быть сужена до задачи обеспечения приемлемого (чуть менее 100%) уровня защиты информации в КОС за счет конечного перечня требований как СИБ КОС, так и ее политик. В таком случае становится технически возможно построение реальной высокоэффективной СЗИ, соответствующей требованиям СИБ и ее политик. Примерами высокоэффективных политик безопасности КОС являются а) политика построения и использования сетей и туннелей VPN, б) политика использования технических средств, направленных на обнаружение вредоносных компьютерных вирусов и их уничтожение, в) политика использования межсетевых экранов (брандмауеров), и др.

Обобщенная методика построения частных решений СЗИ-VPN основана на вышеописанной базовой модели СЗИ-VPN КОС. Задача обобщенной методики заключается в генерации множества траекторий *M* в пространстве безопасности КОС: $O \times S \times R \times AP \times TP \times CP \times УР \times P \times AA \times AC \times AK \times MOD \times PAR$. Каждая генерируемая траектория *M* соответствует частной методике построения решения СЗИ-VPN. Среди всех возможных траекторий из *M* априорно выделяются три подмножества: 1) *Ml* – подмножество легитимных траекторий СЗИ-VPN, 2) *Mn* – подмножество нелегитимных траекторий СЗИ-VPN, 3) *Mr* – подмножество рекомендуемых траекторий СЗИ-VPN, таких что $M = Ml \cup Mn$, $Ml \cap Mn = \varnothing$, $Mr \subseteq Ml$, $Mr \cap Mn = \varnothing$. Определение подмножества *Mr* возможно на основе различных селективных критериев, например, а) по критерию максимальной безопасности доступа к базам данных с конфиденциальной информацией, б) по критерию максимальной производительности передачи данных между хостами или шлюзами КОС, в) по критерию минимального времени инсталляции агента СЗИ-VPN КОС на хосте, и др.

Примеры методик построения решений СЗИ-VPN КОС

Ниже приведены примеры двух легитимных траекторий $m1 \in Mr$ и $m2 \in Mr$, на основании которых были построены и протестированы практические решения СЗИ-VPN систем. Пример 3 описывает нелегитимную методику $m3 \notin Mr$.

Пример 1. Частная методика $m1 \in Mr$, описываемая как *m1 = (AP={3}, TP={4}, CP={1,1-1}, P={5,6}, AA={2}, AC={12,13}, MOD={2}, PAR={N1…Nk})* была использована для построения частного VPN-решения для пользователей с удаленным доступом – онлайн преподавателей и создателей образовательного контента для электронного обучения. При ее построении использовался селективный критерий обеспечения максимальной производительности обмена данными между заданными хостами КОС, находящихся на разных подсетях КОС.

Пример 2. Частная методика $m2 \in Mr$, описываемая как *m2 = (AP={3}, TP={1}, CP={1,1-2}, P={4,7}, AA={2}, AC={2,13}, MOD={2}, PAR={ N1…Nk})* была использована для построения частного VPN-решения для пользователей с удаленным доступом - администраторов университета верхнего и среднего уровней управления университетом. При ее построении использовался селективный критерий обеспечения максимальной безопасности коммуникаций между хостом удаленного администратора университета и базами данных с конфиденциальной информации в КОС.

Пример 3. Частная методика $m3 \in M$, описываемая как *m3 = (AP={3}, TP={4}, CP={1,1-1}, P={6}, AA={2}, AC={3}, MOD={1}, PAR={ N1…Nk})* является нелегитимной в пространстве безопасности СРВ-VPN. Причина заключается в том, что согласно выбранному элементу подмножества *AC={3}* для шифрования данных в данной СЗИ-VPN следует использовать алгоритм шифрования на базе стандарта шифрования DES; однако, в множестве *P={6}* указан протокол аутентифицирующего заголовка АН, который не поддерживает шифрование данных в СЗИ-VPN; поэтому представленная методика *m3* является нелегитимной.

Заключение

Разработанные и описанные выше а) базовая модель системы защиты информации корпоративной образовательной сети на основе сетей и туннелей VPN, б) обобщенная методика построения разнообразных практических решений СЗИ-VPN, в) частные VPN-решения были разработаны, протестированы и успешно применены в корпоративной образовательной сети крупной образовательной организации - университета с тысячами пользователей внутри сети КОС и за ее пределами, тысячами пользовательских компьютеров в лабораториях организации, десятками центральных серверов и серверов отдельных подразделений, и более, чем 20 подсетями в составе КОС. Многочисленные статистические данные мониторинга и ежедневные (еженедельные, ежемесячные) отчеты о безопасности КОС убедительно свидетельствуют о правильности предложенных решений по созданию и разработке моделей и методик построения СЗИ-VPN для КОС крупных образовательных организаций.

СПИСОК ЛИТЕРАТУРЫ:

1. Сердюк В.А. Новое в защите от взлома корпоративных систем. – М.: Техносфера, 2007.
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
3. Guide to IPSec VPNs. Recommendations of the national Institute of Standards and Technology. NIST Specila publication 800-77. – Gaithersburg, U.S.A., 2005.
4. Девянин П.Н. Модели безопасности компьютерных систем. – М.: Издательский центр «Академия», 2005
5. Петров А.А. Компьютерная безопасность: криптографические методы защиты. – М.: ДМК Пресс, 2000.
6. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность. – М.: Издательский центр «Академия», 2005.
7. Rhee M.Y. Internet Security: Cryptographic principles, algorithms, and protocols. – Chichester, England: John Wiley & Sons, 2003.

Усков В.Л., Усков А.В.

ЭЛЕКТРОННОЕ ОБРАЗОВАНИЕ: СТРАТЕГИЧЕСКИЕ ВОПРОСЫ НА 2008-2015 ГОДЫ

uskov@bradley.edu
Бредли университет
г. Пеория

Вступление.

В последнее время во всем мире бурными темпами развивается электронное образование (ЭО), основанное на использовании передовых компьютерных, информационных, сетевых. коммуникационных, коллаборативных и мультимедийных технологий. В связи с этим многие образовательные организации – университеты, колледжи, школы, центры переподготовки кадров, и др. – рассматривают разнообразные модели использования ЭО в своей деятельности.

Известно, что организации ЭО могут выбрать различные модели функционирования, например:

1. принципиально новая учебная организация – виртуальный университет или электронный университет; примерами могут служить а) консорциум «Электронный университет» в Росси на базе университета МЭСИ, б) Capella университет или онлайн университет города Феникса в США, в) университет Атабаска в Канаде, и др.;
2. консорциум организаций-партнеров, договорившихся о создании и использования ЭО как одной из нескольких возможных форм обучения или тренинга, например, группа COIMBRA из более, чем 100 европейских университетов, группа университетов COMPOSTELA, группа университетов Santander, и др.; эта форма функционирования является особенно