УДК 004. 621: 681.3 **Дмитренко А.П., Сирченко Г.А., Хорошко В.А.**

МОДЕЛИ БЕЗОПАСНОГО СОЕДИНЕНИЯ С УДАЛЕННЫМИ ОБЪЕКТАМИ

Сегодня вирусы, хакеры и компьютерные приступники - это только немногие из тех неприятностей, с которыми каждый день сталкиваются службы безопасности организаций, фирм, банков, предприятий и обычные пользователи. И в связи с увеличением числа компьютерных преступлений, особенно при использовании сети Internet и доступа к удаленным объектам, сейчас для специалистов, ответственных за безопасность информации, важно, как никогда, определять, разрабатывать систему безопасности и управлять ею. Предотвращая новые угрозы несанкционированного проникновения в них. Важно также научиться предотвращать и избегать этих угроз в будущем [1].

Для того, чтобы обеспечить грамотное противодействие несанкционированным попыткам в получении информации на коммуникациях и безопасного соединения с различными объектами на разных расстояниях от объекта, необходимо создать модели, которые позволяют провести анализ возможных ситуаций.

Основная часть

При построении модели безопасного удаленного доступа или безопасного соединения с удаленным объектом упор делается на сопоставлении имеющихся защитных средств (активизированных и регулярно используемых) и степени жесткости политики безопасности организации в отношении контроля удаленного доступа (в общем случае контроль доступа подразумевает сохранение целостности информации, доступности и недопущение факта ознакомления с нею в процессе хранения и обработки в самой локальной сети) и соблюдения конфиденциальности информации при ее передаче по незащищенным каналам связи. При этом учитывается статистика случаев несанкционированного доступа (НСД) в локальную сеть (ЛС), имевших место ранее. Ниже приведена таблица показателей, которыми оперирует модель удаленного доступа [2,3].

Модель безопасного модемного соединения

Расчетную вероятность несанкционированного доступа в локальную сеть через модемное соединение можно определить следующим образом:

$$P_{IA}^{M'} = M_{QNT} \cdot M_{INC} \cdot D \cdot P \cdot (1 - M_{ID,AUTEN} \wedge M_{USG}) \cdot (1 - M_{FILTR});$$

где P - вероятность совершения попытки несанкционированного доступа в локальную сеть через коммутируемое соединение. Определяется методом экспертных оценок путем учета статистики проявления внешних угроз в локальных сетях.

D- количество дней в году, в течении которых сеть полностью функционирует и связана с удаленными сетями коммутируемым доступом.

M_{USG} - численный эквивалент синтаксического показателя M_{USG}, принимающий значения: минимальный - 0.3, низкий - 0.5, средний - 0.8, высокий - 0.9, максимальный -0.97.

M_{FILTR}- численный эквивалент синтаксического показателя M_{FILTR}. принимающий значения: минимальный - 0.1, низкий - 0.3, средний - 0.5, высокий - 0.8, максимальный -0.95.

Экспериментальная вероятность несанкционированного доступа в локальную сеть через модемное соединение, определяемая за период функционирования локальной сети, равна:

$$P_{IA}^{M''} = M_{IA} \wedge M_{FREQ} \cdot D \cdot (100 - M_{PER}).$$

Таблица 1. Показатели модели безопасного удаленного доступа

Наименование	Тип	Примечания
Модемное соединение		
M_{QNT}	Численный	Количество модемных линий
$M_{ID\ AUTEN}$	Логический	Наличие встроенных в модем алгоритмов идентификации и аутентификации
M_{USG}	Синтаксический	Степень использования алгоритмов идентификации и аутентификации
M_{INS}	Численный	Среднее число входящих звонков на линию
M_{IMP}	Синтаксический	Важность ресурсов,к которым имеется удаленный доступ
M_{IA}	Логический	Случаи НСД в сеть через модем
M_{FREQ}	Численный	Частота случаев НСД
M_{PER}	Численный	Процесс пересичения НСД в сеть через модем
M_{FILTR}	Логический	Использование средств фильтрации звонков
M_{SEC}	Синтаксический	Степень жесткости политики безопасности модемного соединения
Соединение через роутер		
R_{ACT}	Синтаксический	Степень активности доступа к сети черезWAN
R_{TRST}	Синтаксический	Степень доверия к организациям, имеющих доступ к сети
R_{QLFC}	Синтаксический	Степень квалификации администратора сети
R_{IA}	Логический	Случаи НСД в сети через роутер
R_{FREQ}	Численный	Частота случаев НСД
R_{PER}	Численный	Процесс присечения НСД в сети через роутер
R_{SEC}	Синтаксический	Степень жесткости политики безопасности соединения через роутер
Защита информации в каналах связи		
C_{CHNL}	Логический	Передается ли важная информация по незащищенным каналам связи
C_{VOL}	Синтаксический	Объемы передающейся по каналам
C_{IMP}	Синтаксический	Важность передающейся по каналам
C_{CRIPT}	Синтаксический	Степень использования криптографических
C_{CONF}	Синтаксический	Степень жесткости политики соблюдения конфиденциальности данных
Выход в Internet		
R_{FW}	Логический	Используется ли система Firewall
$R_{FW\text{-}USG}$	Синтаксический	Степень использования защитных средств
$R_{SEC\text{-}MAN}$	Логический	Наличие лица, ответственного за безопасность
K_{AVIR}	Синтаксический	Степень использования антивирусных
K_{JAV}	Логический	Защищен ли прогон Java-апплетов (любых интерактивнх программ)
K_{CERT}	Логический	Загружаются ли станицы только с сертифицированных Web-сайтов
K_{IMPRT}	Синтаксический	Степень контроля за импортом программ
K_{TRN}	Синтаксический	Степень обучения пользователей безопасности

Общая вероятность несанкционированного доступа в локальную сеть через модемное соединение определяется соответственно как:

$$P_{IA}^{M} = P_{IA}^{M'} \cdot (1 - K_{FUNK}) + P_{IA}^{M''} \cdot K_{FUNK},$$

где K_{RINC} - численный коэффициент, учитывающий время функционирования локальной сети, за которое велась статистическая обработка случаев НСД (определялись коэффициенты R_{IA}, R_{FREQ}, R_{PER}). K_{FUNC} соответственно принимает значения: 0 - менее года; 0.2 - от года до двух лет; 0.5 - 2 - 4 года; 0.8 - 4-7 лет; 0.9 - более семи лет.

Как видно из формулы, экспериментальная вероятность (определяемая путем учета статистической обработки случаев НСД за период функционирования локальной сети) имеет тем больший вклад в определение общей вероятности, чем за более длительный срок собраны данные о попытках взлома, и, соответственно, наоборот, при отсутствии продолжительных наблюдений общая вероятность полностью определяется расчетной вероятностью P_{IA}^{M}

Далее рассчитанная вероятность несанкционированного доступа в ЛВС P_{IA}^{M} сопоставляется с синтаксическим показателем $M_{IMP.SEC}$, показателей M_{IMP} и M_{SEC} (см. таблицу показателей).

$M_{IMP.SEC}$	P_{IA}^{M}
Минимальный	>0.15
низкий	0.1-0.15
средний	0.03-0.1
высокий	0.01 - 0.03
Максимальный	<0.01

Рассчитанная вероятность НСД для надежно защищенной сети должна всегда быть ниже приведенной в таблице для соответствующей величины показателя $M_{IMP.SEC}$. На основе разницы рассчитанной величины P_{IA}^{M} и приведенной в таблице определяется необходимый набор защитных средств. При повторном моделировании вероятности НСД с учетом новых показателей стремятся величину P_{IA}^{M} довести до оптимальной в соответствии с таблицей.

Примечание. Вероятности удачной попытки несанкционированного доступа приведены за период времени, равный одному году.

Модель безопасного соединения через роутер

Расчетную вероятность несанкционированного доступа в локальную сеть через роутер по аналогии с модемным соединением можно определить следующим образом:

$$P_{IA}^{R'} = D \cdot P \cdot R_{ACT} \cdot (1 - R_{TRST}) \cdot (1 - R_{QLFC})$$

где P - вероятность совершения попытки несанкционированного доступа в локальную сеть через физическое соединение. Также определяется методом экспертных оценок путем учета статистики проявления внешних угроз в локальных сетях.

R_{ACT} - численный эквивалент синтаксического показателя R_{ACT}, принимающий значения: минимальный - 0.1, низкий - 0.25, средний - 0.5, высокий - 0.85, максимальный - 1.

R_{TRST} - численный эквивалент синтаксического показателя R_{TRST}, принимающий значения: минимальный - 0, низкий - 0.2, средний - 0.4, высокий - 0.6, максимальный - 0.75.

R_{QLFC} - численный эквивалент синтаксического показателя R_{QLFC} принимающий значения: минимальный - 0, низкий - 0.2, средний - 0.5, высокий - 0.8, максимальный -0.95.

Экспериментальная вероятность несанкционированного доступа в локальную сеть через роутер, определяемая за период функционирования локальной сети, равна:

$$P_{IA}^{R''} = R_{IA} \wedge R_{FREQ} \cdot D \cdot (100 - R_{PER})$$

Общая вероятность несанкционированного доступа в локальную сеть через роутер определяется соответственно как:

$$P_{IA}^{R} = P_{IA}^{R'} \cdot (1 - K_{FUNC}) + P_{IA}^{R''} \cdot K_{FUNC}$$

K_{FUNC} соответственно принимает значения: 0 - менее года; 0.2 - от года до дву; лет; 0.5 - 2-4 года; 0.8 - 4-7 лет; 0.9 - более семи лет.

Далее рассчитанная вероятность несанкционированного доступа в ЛВС P_{IA}^{R} сопоставляется с синтаксическим показателем $R_{IMP,SEC}$ определяемого соотношениел показателей R_{IMP} и R_{SEC} (см. таблицу показателей).

$R_{IMP,SEC}$	P_{IA}^{R}
Минимальный	>0.15
Низкий	0.1-0.15
Средний	0.03-0.1
Высокий	0.01 - 0.03
Максимальный	<0.01

Модель защиты информации в каналах связи

Модель предполагает вычисление вероятности нарушения конфиденциальности при передаче информации по незащищенным каналам связи:

$$P_C = C_{CHNL} \wedge P \cdot C_{VOL} \cdot (1 - C_{CRIPT})$$

где P - вероятность перехвата информации в магистральных каналах связи. Она определяется методом экспертных оценок путем учета статистики проявления внешни: угроз в распределенных сетях.

C_{VOL} - численный эквивалент синтаксического показателя C_{VOL}. принимающю значения: минимальный - 0.1, низкий - 0.2, средний - 0.5, высокий - 0.8, максимальный - 1.

C_{CRIPT} - численный эквивалент синтаксического показателя C_{CRIPT}, принимающий значения: минимальный - 0.5, низкий - 0.7, средний - 0.8, высокий - 0.95, максимальный 0.999.

В данной модели не представляется возможным учитывать статистику перехват конфиденциальных сообщений при передаче через магистральные канала связи, т.к. фак перехвата или несанкционированного ознакомления с информацией в распределенных сетя практически установить невозможно. Основной упор в модели делается на применени криптографических средств, позволяющих свести вероятность несанкционированное ознакомления к нулю.

Далее рассчитанная вероятность нарушения конфиденциальности при передач информации по незащищенным каналам связи P_c [4] сопоставляется с синтаксическим показателем $C_{IMP,SEC}$, определяемого соотношением показателей C_{IMP} и C_{SEC} (см. таблиц показателей) подобно предыдущим моделям.

$C_{IMP,SEC}$	P_c
Минимальный	>0.001
Низкий	0.001-0.0001
Средний	0.0001-0.000001
Высокий	0.000001 - 0.000001
Максимальный	<0.0000001

Модель безопасного Internet-соединения

K_{TRN}	K_{JAV}	K_{CERT}	K_{IMPRT}	K_{AVIR}	$R_{SEC-MAN}$	R_{FW-USG}
Низк. 0	да - 1	да - 1	Низк. 0	Низк. 0	да - 1	Низк. 1
Средн.1	нет - 0	нет - 0	Средн.2	Средн. 3	нет - 0	Средн. 4
Высок.3			Высок.4	Высок.5		Высок.7

Модель безопасного Internet-соединения в соответствии со степенью риска локальной сети подразумивает наличие набора защитных средств, скмарный весовой коэффициент которых согласно таблице находится в пределах: низкий риск: 0-3, средний риск: 4-10. высокий риск: более 10.

Выводы

Описанные модели позволяют оптимально регламентировать доступ в локальную сеть из внешних сетей с точки зрения безопасности информации, определить численные значения вероятностей несанкционированого доступа для каждого вида соединения, выбрать на основе полученных данных оптимальный набор защитных механизмов. При оценке вероятностей успешных злонамеренных действий принимается во внимание как перечень существующих средств защиты, так и данные о попытках НДС за время функционирования локальной сети, что позволяет получить более точные вероятностные значения. Модель может применятся как на стадии проектирования сети с возможностью удаленного доступа, так и в процессе ее эксплуатации.

Поступила 4.11.09

УДК 681.51:519.876 **Пархуць Л.Т.**

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ АДАПТИВНОЇ МАРШРУТИЗАЦІЇ З ОБМЕЖЕНИМ ВИБОРОМ ВИХІДНИХ КАНАЛІВ ЗВ'ЯЗКУ

Вступ

При побудові нових та при модернізації існуючих захищених інформаційних мереж спеціального призначення актуальними питаннями, які слід вирішити, є оптимізація архітектури та технології функціонування мережі з метою забезпечення необхідного рівня захисту інформації, отримання максимальної швидкодії та мінімального трафіку. Даним питанням присвячено, зокрема, робота [1], в якій приведено модель процесу обміну інформацією в інформаційній мережі, виконано її моделювання та дослідження [2], розглянуто питання оптимізації структури інформаційних мереж [3]. Схеми глобального і локального управління в інформаційній мережі при обмеженні інтенсивностей потоків проаналізовано в роботі [4]. В роботі [5] запропоновано алгоритми адаптивної маршрутизації в захищеній інформаційній мережі з обмеженим вибором вихідних каналів зв'язку.

Дана робота є логічним продовженням вказаних робіт, зокрема в ній проведено дослідження алгоритмів адаптивної маршрутизації в захищеній інформаційній мережі з обмеженим вибором вихідних каналів зв'язку.

Основна частина

Дослідження ефективності описаних варіантів алгоритмів адаптивної маршрутизації з обмеженим вибором вихідних каналів зв'язку (АМОВВКЗ) [5] проведемо методом імітаційного моделювання. На основі описаної множини варіантів алгоритмів АМОВВКЗ спочатку вибирається кращий у відношенні до прийнятого критерію ефективності, а потім визначаються його оптимальні параметри.

Заздалегідь розглянемо можливості оцінки характеристик варіантів алгоритмів АМОВВКЗ аналітичним методом. При цьому слід враховувати, що аналітичне моделювання накладає достатньо жорсткі обмеження на складність використовуваних моделей і вимагає ухвалення множини допущень, що істотно зменшує адекватність отриманої аналітичної моделі і відповідно відображається на точності і достовірності одержуваних результатів.