информационных ресурсов. Физическое объединение влияет, в первую очередь, на стоимость системы, поскольку одна платформа дешевле нескольких, а технические ресурсы в такой консолидированной системе используются эффективнее.

Практически все основные производители средств защиты предлагают свои решения в этом сегменте, но лидирующие позиции занимают компании Internet Security System (продуктовая линейка Proventia), Symantec (Symantec Gateway Security) и Cisco Systems (Cisco ASA 5500).

Выводы

Полная защита целостности сети возможна при реализации таких компонентов защиты: политика безопасности интрасети организации, система защиты хостов в сети, сетевой аудит, защита на основе маршрутизаторов, межсетевые экраны, системы обнаружения вторжений, план реагирования на выявленные атаки.

Тенденции на рынке информационной безопасности, стремятся к объединению различных средств защиты. Это делает подобные объединенные устройства более гибкими при внедрении в информационные системы и намного упрощает процесс установки и эксплуатации.

Одной из основных наиболее эффективных схем защиты на данном уровне развития технологий информационной безопасности, является схема, сочетающая в себе интеграцию аппаратной платформы, межсетевого экрана и системы обнаружения и предотвращения вторжений, использующей сигнатурный и поведенческий анализ.

Поступила 29.03.2007 г.

УДК 681.14

Мухин В.Е., Стретович Е.Н.

АДАПТИВНОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ

Введение

Современные компьютерные сети (КС) – разнообразная и весьма сложная совокупность устройств, телекоммуникационных технологий, программного обеспечения и высокоэффективных средств его проектирования. Развитие компьютерных информационных технологий приводит к тому, что все более критичными становятся надежность и безопасность ресурсов сетей, выполняющих сбор, накопление, обработку, передачу и хранение данных. В последнее время появились новые проблемы обеспечения безопасности компьютерных сетей, которые в значительной степени определяют эффективность создаваемых компьютерных сетей.

Реализация средств защиты информации в КС требует дополнительных аппаратных, программных и, как следствие, временных затрат на обработку информации. Повышение уровня защищенности КС вызывает рост удельного объема дополнительной (служебной) информации передаваемой и обрабатываемой в компьютерных сетях, что обуславливает снижение пропускной способности сети по передаче полезной (пользовательской) информации. С другой стороны, в общем случае оказывается, что нет необходимости поддерживать уровень защищенности КС постоянно максимально высоким. В те периоды времени, когда в сети обрабатываются менее критичные данные, вполне допустимо снизить уровень ее защищенности, что обеспечит снижение объема служебной информации и повышение пропускной способности сети по передаче пользовательских данных. Таким

образом, возникает необходимость в реализации механизма управления безопасностью КС, который будет гибко определять требуемый в данный момент времени уровень защищенности КС, что обеспечит повышение эффективности функционирования всей КС. Таким механизмом является адаптивное управление безопасностью – подход, который обеспечивает гибкую установку требуемого в данный момент уровня защищенности КС на основе контроля, обнаружения и реагирования в реальном времени на угрозы безопасности с использованием специальных комплексных методов и средств.

1. Средства адаптивного управления безопасностью компьютерных сетей

Для реализации концепции адаптивного управления безопасностью компьютерных сетей разработаны средства адаптивного управления безопасностью, состоящие из следующих компонентов: средства анализа защищенности; средства обнаружения атак; средства адаптации; средства управления.

Средства анализа защищенности выполняют поиск уязвимых мест в сети и оценку затрат на реализацию уязвимостей. Технологии анализа защищенности строятся на основе методов, позволяющих реализовать политику сетевой безопасности прежде, чем осуществится попытка ее нарушения.

Средства обнаружения атак выполняют оценку подозрительных действий, происходящих в компьютерных сетях.

Средства адаптации определяют требуемый уровень защищенности компьютерных сетей в данный период времени с учетом важности (ценности) обрабатываемой информации.

Средства управления координируют работу всей адаптивной системы управления безопасностью компьютерной сети.

Таким образом, система адаптивного управления безопасностью КС – это комплексный механизм управления, обеспечивающий в реальном времени требуемый уровень защищенности с учетом важности обрабатываемых данных в компьютерной сети.

2. Подходы к построению средств адаптивного управления безопасностью компьютерных сетей

В настоящее время существует два основных подхода к построению средств адаптивного управления безопасностью КС:[1]

1. адаптивные систем управления безопасностью с эталонной моделью;
2. адаптивные системы управления безопасностью с идентификатором.

Для эффективного управления безопасностью КС предлагается использовать адаптивное управление безопасностью на основе эталонной модели, при этом в качестве эталонной модели выступают профили (шаблоны) безопасности, т.е. параметры конфигурации безопасности сети. База профилей безопасности собирается предварительно на основе экспериментальных данных о функционировании системы защиты КС. [2]

Структурная схема предлагаемой системы адаптивного управления безопасностью на основе профилей безопасности показана на рис. 1.

Рассмотрим особенности функционирования данной системы. В том случае, когда параметры безопасности компьютерной сети постоянны, ошибка регулирования равна: $\Delta = y_m - y_p = 0$, средства адаптации находятся в т.н. "спящем" режиме. Если параметры системы безопасности КС изменяются (как реакция на изменение уровня защищенности обрабатываемой информации), то возникает ошибка регулирования $\Delta = y_m - y_p \neq 0$, инициализируются средства адаптации системы защиты КС, с тем чтобы привести функционирование системы защиты информации к требуемым параметрам. Таким образом, задача средств адаптации состоит в том, что они должны свести ошибку регулирования к нулю $(\Delta \to 0)$.

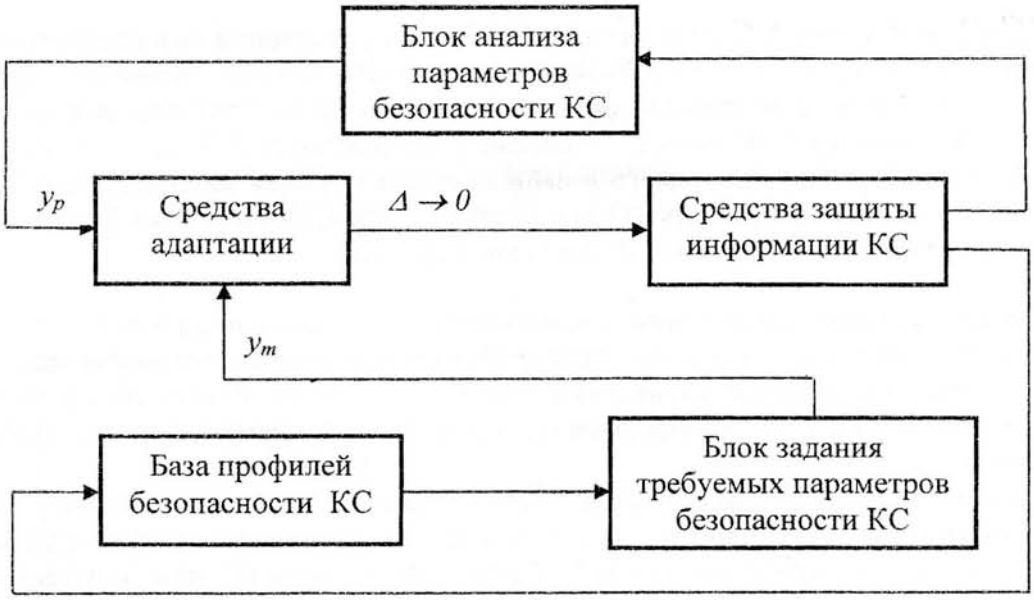

Рис. 1. Система адаптивного управления безопасностью с использованием профилей безопасности

3. База профилей безопасности компьютерной сети

Фактически, профиль безопасности – это набор параметров системы защиты КС, на основании которого определяется требуемый уровень безопасности компьютерной сети с учетом критериев оценки защищенности информации. [3] К числу функциональных критериев оценки уровня защищенности в соответствии с ISO 15408 "Общие критерии оценки безопасности информационных технологий" относятся: аудит безопасности (FAU: security audit); связь (FCO: communication); криптографическая поддержка (FCS: cryptographic support); защита данных пользователя (FDP: user data protection); идентификация и аутентификация (FIA: identification and authentication); управление безопасностью (FMT: security management); секретность (FPR: privacy); защита функций безопасности ПОБ (FPT: protection of the TSF); использование ресурсов (FRU: resource utilisation); доступ к ПОБ (FTA: TOE access); надежный маршрут/канал (FTP: trusted path/channels). [4]

Кроме функциональных критериев в ISO 15408 также выделены критерии гарантии безопасности, позволяющие оценить корректность реализации услуг по обеспечению безопасности, такие как: управление конфигурацией (ACM: configuration management); поставка и функционирование (ADO: delivery and operation); разработка (ADV: development); руководящие документы (AGD: guidance documents); жизненный цикл (ALC: life cycle support); испытания (ATE: tests); оценка уязвимых мест (AVA: vulnerability assessment).

Таким образом, критерии оценки безопасности КС определяются на основе совокупности требований к механизмам обеспечения безопасности, оценки их эффективности и доверия к ним при использовании.

Задача адаптивного управления безопасностью КС эффективно решается только на основе полной информации о состоянии системы безопасности КС и параметров самой сети. [5,6] Таким образом, для обеспечения адаптивного управления безопасностью КС необходимо использовать не только количественные, но и качественные критерии безопасности КС.

Для принятия решений по управлению безопасностью КС, с учетом вышеперечисленных требований предлагается использовать аппарат нечеткой логики. Профили безопасности вносятся в базу знаний и на основании нечеткого логического вывода принимаются решения по управлению безопасностью КС.

4. Алгоритм адаптивного управления безопасностью компьютерных сетей на основе аппарата нечеткой логики

В настоящее время не существует дискретных алгоритмов, оперирующих одновременно качественными и количественными знаниями для получения однозначных решений. Функциональные (качественные) критерии оценки уровня защищенности КС не могут быть адекватно формализованы без применения аппарата нечеткой логики. Применение теории нечетких множеств позволяет формализовать процесс принятия решений также в многомерной нечеткой среде.

Математическое описание параметров безопасности компьютерных сетей на основе теории нечетких множеств позволяет эффективно формализовать и исследовать многие не только количественные, но и качественные события, оценки безопасности компьютерных сетей путем представления их в виде: $\forall x \in X \quad A = \{(x, \mu_A(x)\}$, где $(x, \mu_A(x))$ пара компонентов (синглтон), составленная из элемента x и степени его принадлежности $\mu_A(x)$ к множеству X. [7,8]

Для формализации функциональных критериев оценки уровня защищенности КС предлагается применять аппарат лингвистических переменных. В общем случае, лингвистическая переменная характеризуется набором из компонентов: $\langle x, T, D \rangle$, где x – имя лингвистической переменной, T – ее терм-множество или множество ее значений, D – область определения значений. [9,10]

Принцип построения средств управления безопасностью КС на основе нечеткой логики состоит в реализации синтеза теории планирования экспериментов и теории нечетких множеств.

Функциональные критерии оценки уровня защищенности КС (например, знания и опыт экспертов) формализуются в виде полинома:

$$Y = \beta_0 + \sum_{i=1}^{n} \beta_i x_i + \sum_{u,j=1}^{n} \beta_{ju} x_j x_u, \quad j \neq u, \tag{1}$$

где Y – зависимая лингвистическая переменная (критерий), β_i – правый нечеткий коэффициент, x_i – имя лингвистической переменной.

Продукционные правила на основе функциональных критериев оценки уровня защищенности КС в некоторой точке факторного пространства носят импликативную форму «Если…, то…, иначе…», а набор продукционных правил составляет ортогональную матрицу типа 2^n, где n – размерность факторного пространства.

Предлагается алгоритм построения прогностической модели управления безопасностью КС с формализацией функциональных критериев в многомерном пространстве.

Алгоритм состоит из следующих шагов:

1. Определение факторного пространства задачи управления безопасностью КС.
2. Определение границ оппозиционной шкалы и термов по каждому фактору.
3. Формирование матрицы функциональных критериев оценки уровня защищенности КС.
4. Генерация лингвистических переменных для формализации качественной информации о событиях безопасности компьютерных сетей.
5. Расчет коэффициентов полинома формализации функциональных критериев безопасности КС по (1).
6. Оценка ошибки численного эксперимента по управлению безопасностью КС.
7. Оценка адекватности полученного полинома (1) для системы управления безопасностью КС.
8. Оценка точности модели управления безопасностью по критерию Фишера как:

$$F_{критФ} = S^2_{ост} / S^2_{осн} < F_{табл} \tag{2}$$

Таким образом, предлагаются средства управления безопасностью КС на основе формализации функциональных требований к обеспечению безопасности КС в виде прогностических моделей в многомерном пространстве. Решения по управлению безопасностью КС принимаются путем точных решений нечетких уравнений.

Значением нечеткой функции $F(x_1, x_2, .., x_n)$ от нечетких чисел $x_1, x_2, ..., x_n$ является нечеткое множество с функцией принадлежности $\mu_F(t)$:

$$\mu_F(t) = \begin{cases} \sup \min\left[\mu_X(x), \mu_A(a_1), ..., \mu A(a_n)\right] \\ F(x_1, ..., x_r) = t \\ 0, F(t)^{-1} = \varnothing \end{cases}, \qquad (3)$$

Согласно принципу расширения Заде нечеткое число x является решением нечеткого уравнения $F(x, A_1, ..., A_n) \subseteq B$, если $\forall t$ таких что:

$$F^{-1}(t) = \phi, \ \mu_F(t) = \sup_{F(x, a_1, ..., a_n) = t} \min\left[\mu_X(x), \mu_A(a_1), ..., \mu A(a_n)\right], \qquad (4)$$

где $F(x, A_1, ..., A_n)$ – значение нечеткой функции от нечетких чисел, $A_1, ..., A_n, B$ – известные нечеткие числа, x – неизвестное нечеткое число, $\mu_F(t)$ – степень принадлежности x к множеству чисел B.

5. Анализ параметров функционирования средств защиты информации в компьютерных сетях

Проведем анализ функционирования средств защиты информации в КС двух различных типов: первый – средства защиты, поддерживающие фиксированный уровень защищенности сети, второй – средства защиты с использованием механизма адаптивного управления безопасностью сети.

Рассмотрим, каким образом изменяется во времени уровень защищенности $Y(t)$ компьютерной сети, в которой реализованы средства защиты первого и второго типа. Для оценки данного параметра сформируем вектор событий безопасности в компьютерной сети $S = <S_1, ..., S_n>$, элементами S_i которого являются следующие события безопасности в сети:

- количество попыток ввода пароля;
- длительность сеанса работы пользователя, мин.;
- время использования пароля, суток;
- количество попыток обращений к защищенным сетевым ресурсам;
- количество отправленных пользователем сообщений ;
- количество попыток запуска критичных программ;
- количество попыток модификации системных файлов.

Далее, на основании отслеживания событий безопасности в 100 сеансах работы пользователей сформируем матрицу событий безопасности, пример фрагмента которой представлен на рис.2.

В этой матрице введен вектор взвешенных оценок событий безопасности в КС V, элементы которого рассчитываются как:

$$V_i = \sum_{i=1}^{n} w_i S_i \qquad (5)$$

где w_i – весовой коэффициент опасности i-того действий для реализации вторжения в КС, причем $\sum_{i=1}^{n} w_i = 1$, и для рассматриваемого случая $n = 7$.

Далее, для повышения наглядности полученных данных, проведем кластеризацию вектора V по пять значений в кластере. В результате получим 20 значений кластеризованного

вектора взвешенных оценок, элементы V_{5i} которого рассчитываются как среднее арифметическое:

$$V_{5i} = \sum_{j=5i-4}^{5i} V_j / 5, \quad i = 1..20. \tag{6}$$

N	S_1	S_2	S_3	S_4	S_5	S_6	S_7	V
1	3	3	20	4	19	2	4	4.32
2	2	6	37	5	4	1	2	3.05
3	3	32	29	4	11	0	2	3.15
4	2	15	18	7	4	1	4	4.47
5	3	57	19	2	12	0	4	3.53
6	1	16	36	2	18	4	1	2.35
7	0	58	21	1	4	1	3	2.14
8	5	50	17	0	12	1	0	1.51
9	2	36	3	2	6	4	1	1.98
10	1	22	34	1	19	3	1	2.03
.	.	.	.	.	.	.	.	...
90	5	22	23	9	18	3	5	6.65
91	3	38	2	6	14	2	1	3.45
92	4	41	13	1	4	5	2	2.49
93	3	32	35	2	8	1	4	3.43
94	1	37	15	7	13	1	3	4.28
95	2	45	7	9	19	2	2	4.86
96	4	29	38	8	18	4	4	5.93
97	2	12	22	6	14	2	2	3.74
98	5	21	10	5	15	3	3	4.42
99	4	39	21	8	16	3	1	4.42
100	3	42	25	2	8	0	3	2.91

Рис. 2. Матрица событий безопасности в компьютерной сети

Требуемый уровень защищенности компьютерной сети $Y(t)$ в кластеризованном виде $Y_{5i}(t)$ определяется как:

$$Y_{5i} = V_{5i} / V_{5\max}, \quad i = 1..20, \tag{7}$$

где V_{5max} – максимально возможное значение вектора V в кластере, которое соответствует значению для средств защиты информации с фиксированным уровнем защищенности. Уровень защищенности удобно представлять в процентном отношении.

На основании полученных результатов построим график изменения уровня защищенности компьютерной сети $Y_{5i}(t)$ во времени для средств защиты информации с фиксированным уровнем защищенности и средств защиты с использованием механизма адаптивного управления безопасностью (рис.3).

В общем случае, системы защиты информации контролируют около 75% подозрительных и опасных событий, таким образом, будем считать, что уровень вычислительных затрат на реализацию функций защиты $Z(t)$ связан с уровнем защищенности компьютерной сети $Y(t)$ с масштабирующим коэффициентом $k = 0{,}75$, т.е. оценивается как:

$$Z(t) \div k * Y(t) \tag{8}$$

Как видно из рис. 3 в средствах защиты информации первого типа уровень защищенности остается постоянным на всем интервале наблюдения, причем для гарантирования безопасности обработки данных этот уровень должен быть максимально высоким. Как следствие, вычислительные затраты на защиту информации также постоянно находятся на максимальных значениях (рис. 4).

Рис. 3. Изменение уровня защищенности компьютерной сети во времени для средств защиты информации первого и второго типа

При применении средств защиты информации второго типа (на основе механизма адаптивного управления безопасностью) уровень защищенности КС постоянно изменяется в зависимости от требуемой степени безопасности обрабатываемой в данный момент информации, при этом достаточно часто уровень защищенности оказывается ниже максимально возможного (рис. 3). В результате, вычислительные затраты на реализацию средств защиты информации второго типа также постоянно изменяются, при этом среднее значение затрат оказывается ниже, чем для систем первого типа (рис. 4).

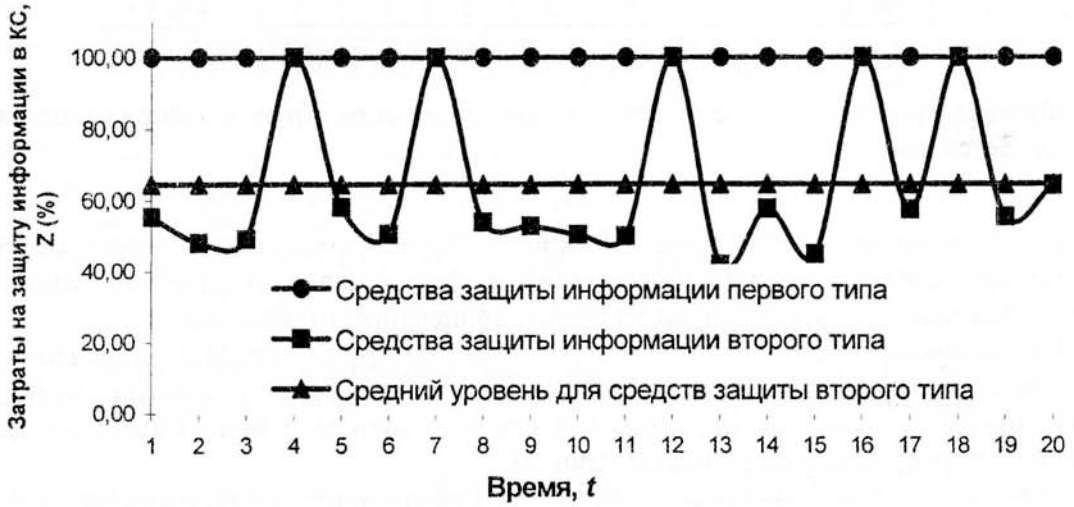

Рис.4. Изменение вычислительных затрат в КС на реализацию функций защиты для средств защиты информации первого и второго типа

Таким образом, производительность обработки пользовательских данных в компьютерных сетях, в которых применяются системы защиты информации с механизмом адаптивного управления безопасностью оказывается выше, чем в случае использования обычных средств защиты информации с фиксированным уровнем защищенности за счет снижения вычислительных затрат на реализацию функций защиты информации, что подтверждает эффективность предложенного подхода к построению средств защиты информации.

Заключение

Реализация средств защиты информации на основе механизма адаптивного управления безопасностью позволяет гибко определять требуемый в данный момент времени уровень защищенности компьютерной сети, что обеспечивает снижение усредненных потерь производительности компьютерных сетей по обработке пользовательских данных. Повышение эффективности функционирования средств защиты информации с адаптивным механизмом управления безопасностью компьютерных сетей достигается за счет применения аппарата нечеткой логики, позволяющего, в частности, формализовать функциональные критерии уровня защищенности компьютерных сетей.

Список литературы

1. *А.А. Жданов, А.В. Рядовиков.* Нейронные модели в средствах адаптивного управления// Оптическая память и нейронные сети, Т. 9, N 2, 2000. – с. 115-132.

2. Guide for Production of Protection Profiles and Security Targets: N2449 Draft v0.9. – ISO/JTC1/ SC27, 2000.

3. *A. Lee.* Certificate Issuing and Management Components Family of Protection Profiles. Version 1.0. – U.S. National Security Agency, October 31, 2001.

4. Standard ISO 15408: "The common criteria for information technology security evaluation". – ISO Standards Bookshop.

5. *G. Stoneburner.* CSPP-OS: COTS Security Protection Profile – Operating Systems: Draft Version 0.4. – U.S. Department of Commerce, NIST, February 5, 2001.

6. *M. Sheridan, E. Sohmer, R. Varnum.* A Goal VPN Protection Profile For Protecting Sensitive Information. Release 2.0. – U.S. National Security Agency, 10 July, 2000.

7. *А. Ротштейн, Д. Катефников.* Идентификация нелинейных объектов на основе нечетких знаний.// Кибернетика и системный анализ, N 5 (34), 1998. – с. 67 -78.

8. *M. Negnevitsky.* Artificial intelligence: a guide to intelligent systems. Addison-Wesley, NY, 2002. – 325 p.

9. *Г.Ф. Нестерук, М.С. Куприянов.* Нейронные системы с нечеткими связями// сб. трудов VI-ой междунар. конференции SCM'2003. – С.Пб, Т.1., 2003. – с. 341-344.

10. *А.В. Спесивцев.* Управление рисками чрезвычайных ситуаций на основе формализации экспертной информации. СПб., Изд-во Политехнического университета, 2004. – 238 с.

Поступила 18.05.2007 г.

УДК 681.327.8

Клименко В.О.

КОНЦЕПТУАЛЬНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ ОРГАНІЗАЦІЇ ПОВІТРЯНОГО РУХУ

Постановка задачі

Звісно [1-7], що проблема безпеки послуг організації повітряного руху (ОрПР) розглядається у двох площинах – як забезпечення *безпеки (safety)* функціонування систем ОрПР у нормальних умовах експлуатації і як *захист (security)* систем ОрПР в умовах зростаючої агресивності середовища експлуатації.

Безпека системи ОрПР досягається за умови забезпечення безпеки всіх ресурсів, які використовуються при наданні послуг ОрПР. Тому до переліку задач захисту системи ОрПР повинні входити задачі забезпечення захисту інформаційних ресурсів системи ОрПР [8]. Проте, незважаючи на вельми високу актуальність, проблема захисту інформаційних