УДК 621.34

С.Г. Семенов

Национальный технический университет «ХПИ», Харьков

МЕТОДИКА НАСТРОЙКИ ПАРАМЕТРОВ РАСПРЕДЕЛЕНИЯ ДОСТУПА И ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Представлены методические рекомендации по настройке параметров распределения доступа и защиты информации в компьютерных системах критического применения (КСКП). Разработана имитационная модель системы распределения доступа и защиты информации в КСКП. Представлена методика выбора рационального варианта настройки параметров КСКП. Произведена оценка эффективности разработанных моделей и методов распределения доступа и защиты информации в КСКП в условиях внешних воздействий.

Ключевые слова: *компьютерная система критического применения, внешние злоумышленные воздействия, распределение доступа, защита информации.*

Введение

В ходе ряда исследовательских работ, направленных на решение актуальной научно-технической задачи обеспечения гарантированного уровня безопасности в КСКП были разработаны модели и методы распределения доступа и защиты информации. Данная статья посвящена разработке методических рекомендаций по использованию моделей и методов распределения доступа и защиты информации в КСКП и оценке эффективности разработанных моделей и методов

1. Имитационная модель системы распределения доступа и защиты информации в КСКП. Для оценки эффективности методов распределения доступа и защиты информации в КСКП и обоснования дос-

товерности полученных результатов проведем имитационное моделирование систем идентификации и адаптивного управления безопасностью в КСКП. В качестве инструментария имитационного моделирования используем среду символьной математики *MathCAD* -14, специализированные программы формирования «квазициклов» и вычисления *BDS*-статистики, сбора параметрической информации КСКП и принятия решения о состоянии системы [3, 7]. Обобщенная структурная схема разработанной имитационной модели систем идентификации и адаптивного управления безопасностью в КСКП представлена на рис. 1.

Из рисунка видно, что данные для статистической оценки состояния КСКП для разделения по группам и категориям и идентификации входного трафика поступают из подсистемы регистрации текущего состояния КСКП и стандартного программного анализатора трафика (например «*Wireshark*») [2].

Проведенные исследования [2-6]показали, что в разработанной имитационной модели основой подсистемы структурной идентификации КСКП являются анализатор наблюдаемого структурно-информационного пространства, усовершенствованная подсистема *BDS*-тестирования и подсистема оценки статистических свойств.

В реализованной имитационной модели подсистемы структурной идентификации трафика формируются наблюдаемые структурно-информационные портреты КСКП. На основании полученных данных с помощью реализованной в имитационной модели усовершенствованной подсистемы *BDS*-тестирования осуществляется структурная идентификация информационного трафика [3, 7].

Проведенный анализ и исследования показали, что основой системы адаптивного управления безопасностью КСКП являются подсистемы установки первоначальных параметров, обнаружения аномалий КСКП и распределения доступа к ресурсам КСКП [4]. Входными данными для указанных подсистем являются в первую очередь вероятностно-временные характеристики определяющие состояние системы (множество X), так же статистические данные о поведении информационного потока различных телекоммуникационных служб [4, 5].

Функционирование всех приведенных подсистем имеет целью реализацию принципа рационального распределения сетевых ресурсов с учетом текущего состояния КСКП и требований гарантированной безопасности к ним.

2. Выбор рационального варианта настройки параметров КСКП. В ходе управления безопасностью КСКП при решении задачи выбора варианта настройки используется результат идентификации системы, а также различные целевые функциональные характеристики КСКП. В КСКП также присутствует множество параметров, определяющих работу ее средств распределения доступа и механизмов защиты (права доступа, метки безопасности и др.), а для достижения безопасной конфигурации параметров КСКП существует множество способов настройки этих параметров. Возникает задача выбора рационального варианта настройки параметров. Важность этой задачи обусловлена необходимостью уменьшения вероятности возникновения ошибок в соответствующих настройках, которая напрямую зависит от количества элементарных операций, необходимых для ее выполнения настроек (сложности настроек КСКП). Поэтому при управлении безопасностью КСКП необходимо выбрать такой способ настройки параметров, который требует минимального количества операций, т.е. уменьшает сложность выполнения действия по настройке параметров [1]. Настройка безопасности должна быть инвариантна по отношению к способам настройки и должна соответствовать критерию безопасности. Проведенные исследования и опыт практической эксплуатации компьютерных систем, показал, что процесс настройки параметров безопасности КСКП должен удовлетворять следующим критериям: минимальная сложность начальной установки параметров КСКП; минимальная сложность модификации пара-

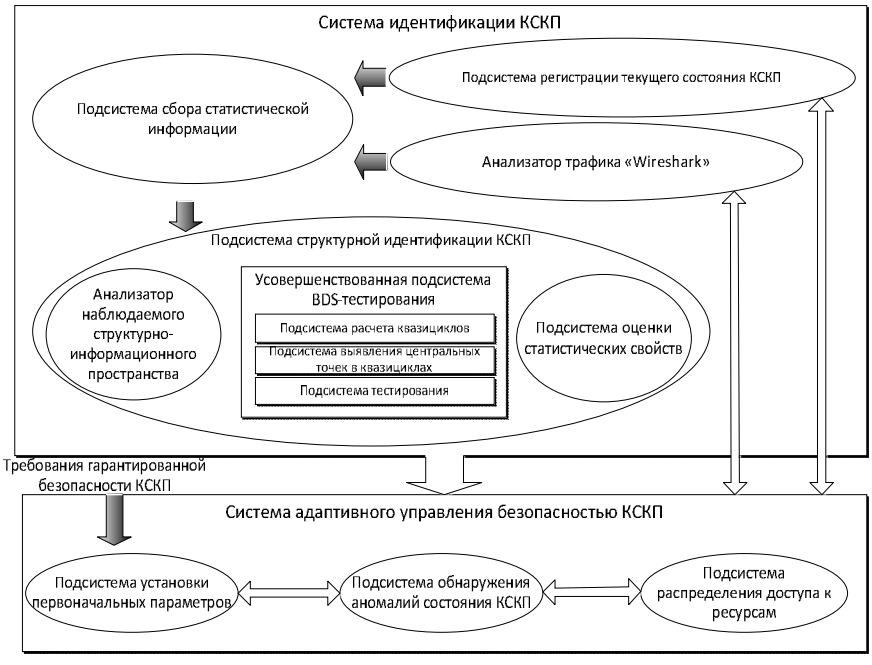

Рис. 1. Обобщенная структурная схема разработанной имитационной модели систем идентификации и адаптивного управления безопасностью КСКП

метров в связи с изменением набора объектов; минимальная сложность групповой настройки объектов; минимальная сложность модификации параметров в связи с изменением набора субъектов; минимальная сложность настройки сетевого взаимодействия. Выполнение каждого из перечисленных критериев достигается использованием различных способов задания параметров [1]. В табл. 1 приведены примеры сопоставления критериев и соответствующих способов задания параметров.

Таблица 1

Соответствие критериев выбора рационального варианта и способов настройки параметров

Критерий выбора рационального варианта	Способ настройки
Сложность начальной установки параметров	Установка привилегий пользователей, настройка локальной политики безопасности
Сложность модификации параметров в связи с изменением набора объектов	Задание прав доступа непосредственно к каждому объекту
Сложность групповой настройки объектов	Установка прав доступа с включенным наследованием (распространение прав доступа по иерархии объектов)
Сложность модификации параметров в связи с изменением набора субъектов	Установка привилегий пользователей, назначение прав доступа к объектам группам пользователей
Сложность настройки сетевого взаимодействия	Настройка локальной политики безопасности

Как показано в табл. 1, способы задания параметров, удовлетворяющие различным критериям, пересекаются лишь частично. Например, минимальная сложность модификации параметров в связи с изменением набора объектов (критерий №2), достигается установкой прав доступа непосредственно к каждому конкретному объекту. Однако данный способ не позволяет проводить групповую настройку объектов (не выполняется критерий №3).

Следовательно, для КСКП изначально не существует такого способа настройки, который полностью удовлетворял бы каждому критерию.

В этой связи необходимо решить задачу поиска рационального варианта безопасной настройки КСКП, основанного на методе многокритериальной (векторной) оптимизации (пример критериев для решения указанной задачи приведен в табл. 2) [1].

Анализ аналитических методов многокритериальной оптимизации показывает применимость для решения данной задачи следующих методов: метод весовых коэффициентов [1, 3] (свертки в суперкритерий); метод эпсилон-ограничений [1]; метод последовательных уступок [1, 6]. Результаты сопоставления перечисленных методов сведены в табл. 2.

Проведенные исследования показали, что метод весовых коэффициентов имеет ряд преимуществ (позволяет учитывать важность частных критериев, не требуя их упорядоченности, а также свести многокритериальную задачу к однокритериальной), что подтверждает целесообразность его использования на практике. Основным недостатком данного метода является отсутствие обязательной упорядоченности критериев, в связи с чем возникает сложность назначения весов для частных критериев [1], однако, он устраним путем определения коэффициентов на основании известных характеристик КСКП.

Таблица 2

Сопоставление методов многокритериальной оптимизации

Критерий сопоставления	Метод весовых коэффициентов	Метод эпсилон-ограничений	Метод последовательных уступок
Использование относительной важности критериев	+	—	+
Сводимость к однокритериальной задаче	+	+	—
Необходимость нормализации критериев	+	—	+
Обязательная упорядоченность критериев	—	—	+

Рассмотрим в качестве примера КСКП, для которой весы критериев задаются в зависимости от ее назначения, и при этом используются частные критерии, перечисленные в табл. 2. Пусть все частные критерии имеют одинаковый масштаб и потому не нуждаются в нормализации. Использование многокритериальной оптимизации позволяет решить задачу выбора эффективного способа настройки безопасности. Представим каждый критерий в виде целевой функции $f(x)=F$, областью определения $(x \in X)$ которой являются полномочия субъектов системы, а областью допустимых значений $(F \in N)$ – сложность их установки соответствующим данному критерию способом. Тогда задача многокритериальной оптимизации в общем случае представима в виде системы экстремумов

$$\min\{ f_i(x) = F_i \}, \quad i \in [1,5],$$

где $f_i(x)$ и F_i – целевая функция и ее значение для i-го критерия, а свертка векторного критерия в суперкритерий – $\Phi(x) = \sum_i^5 a_i f_i(x), a_i \in N$.

Предлагаются следующие способы вычисления целевых функций, используемых в качестве показателей сложности настройки (частных критериев суперкритерия):

– сложность начальной настройки параметров, где $f_1(x) = \sum_{j=1}^{N_O} P(O_j) \Big/ N_O$; N_0 – количество объектов в КСКП; $P(O_j)$ – количество пользователей, которым назначены разрешения на доступ j-му объекту;

– сложность модификации параметров в связи с изменением набора объектов $f_2(x) = R(O)$, где $R(O)$ – среднее количество вспомогательных пара-

метров, необходимых для корректировки полномочий доступа к одному объекту;

– сложность групповой настройки объектов $f_3(x) = N_S \sum_{j=1}^{N_O} A_{ni}(O_j) \Big/ N_O$, где $A_{ni}(O_j)$ – количество прямых полномочий, установленных к j-му объекту; N_S – количество субъектов;

– сложность модификации параметров $f_4(x) = E(S)$, где $E(S)$ – среднее количество вспомогательных настроек, необходимых для корректировки количества участвующих в системе субъекта

– сложность настройки сетевого взаимодействия $f_5(x) = N_{net}/N_s$ – количество сетевых настроек, значения которых определены в КСКП.

При решении задачи настройки безопасности КСКП выбор a_i производится, исходя из назначения системы и практики ее использования, на основании таких факторов, как частота обновлений и установки ПО, создание/удаления пользователей, изменения их полномочий [1]. Способы выбора весовых коэффициентов a_i, различные. Одним из них является назначение a_i, в зависимости от относительной важности критериев. Чем "важнее" критерий, тем больше он должен влиять на общую сложность настройки безопасности. При решении задачи настройки безопасности КСКП процедура выбора "важности" (соответственно, веса a_i) может быть возложена на администратора безопасности системы, который определит относительную важность каждого критерия, исходя из назначения системы и практики ее использования, на основании таких факторов, как, например, частота обновления и установки нового ПО, появления новых/удаления старых пользователей, изменения их полномочий и т.д.

В табл. 3 приведен пример распределения весовых коэффициентов $(a_i \in [1;10])$ для систем различного типового назначения.

Рассмотрим пример выбора оптимального способа настройки параметров КСКП на примере файл-сервера с использованием указанных в табл. 4 типовых весов. Общая сложность настройки параметров файлового сервера рассчитывается как

$$\Phi = 4f_1 + 4f_2 + 10f_3 + 9f_4 + 9f_5 .$$

Это означает, что при настройке параметров файл-сервера необходимо в первую очередь использовать права доступа с распространением по иерархии объектов при помощи механизма наследования (критерий 3). Права доступа необходимо назначать группам, а не отдельным пользователям (критерий 4). Также необходимо настроить локальную политику безопасности (критерий 5). Права доступа для отдельных пользователей (критерий 2) и привилегии субъектов (критерий 1) следует использовать только в случаях, когда полномочия невозможно настроить указанными выше способами.

Таблица 3

Пример распределения весовых коэффициентов для типовых компонент КСКП

Назначение	Весовой коэффициент а				
	Кр. 1	Кр. 2	Кр. 3	Кр. 4	Кр. 5
Файловый сервер	4	4	10	9	9
Сервер баз данных	1	10	2	9	10
Рабочая станция секретаря	9	8	8	1	3
Рабочая станция тестера	2	9	3	7	5
Рабочая станция аналитика	7	8	6	4	5

При выполнении настройки КСКП согласно требованиям оптимальной настройки, безопасность такой системы становится более высокой, а сложность процесса администрирования – более низкой. Использование численных оценок частных критериев позволяет применить предложенный подход при реализации программных средств, выполняющих настройку параметров автоматически, для оценки эффективности и результативности управления безопасностью КСКП.

Таким образом, разработанная имитационная модель систем идентификации и адаптивного управления безопасностью КСКП осуществлять сбор и статистическую оценку данных о состоянии КСКП, а так же входного информационного потока, идентифицирует КСКП, выявляет аномалии в ее поведении и производит перераспределение доступа к ресурсам КСКП исходя из данных о состоянии системы. Результаты имитационного моделирования позволят оценить эффективность моделей и методов распределения доступа и защиты информации в КСКП.

2. Оценка эффективности разработанных моделей и методов распределения доступа и защиты информации в КСКП. Используя методы и приемы математического и имитационного моделирования оценим эффективность разработанных моделей и методов распределения доступа и защиты информации в КСКП, проведем сравнительные исследования с известными методами.

Для подтверждения эффективности разработанного метода по сравнению с методами, основанным на принципах ролевого и мандатного доступа, представим графики (рис. 2) зависимости времени функционирования системы в безопасном режиме $T_{без}$ от отношения интенсивности злоумышленной атаки $I_{атаки}$ к интенсивности входного потока $I_{сд}$ санкционированных данных (на примере *Dos*-атаки – участок 4, *MAC - flooding* -атаки – участок 3, *R2L*-атаки – участок 2 и *Probe* -атаки – участок 1).

На графике рис. 2 представлено семейство кривых зависимости $T_{без}$ от $I_{атаки}/I_{сд}$ в условиях использования разработанных моделей и методов распределения доступа и защиты информации (кривая 1), метода мандатного распределения доступа (кривая 2) и метода ролевого распределения доступа (кривая 3).

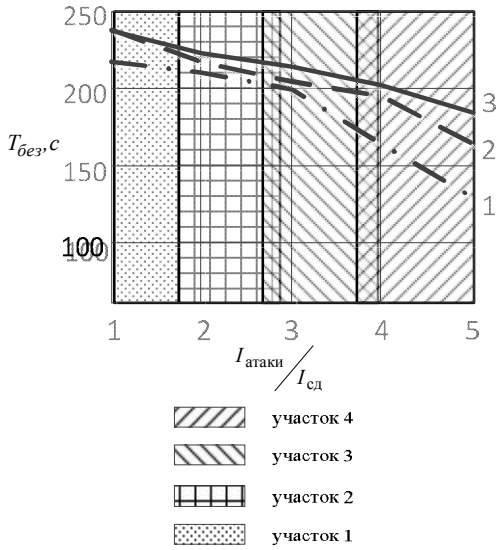

Рис. 2. Зависимость времени $T_{без}$ от отношения интенсивностей $I_{атаки}/I_{сд}$

Как видно в целом из рис. 2 существует четкая тенденция снижения уровня времени функционирования системы в безопасном режиме при увеличении интенсивности атаки. В то же время рис. 2. иллюстрирует преимущества разработанных моделей и методов распределения доступа и защиты информации в КСКП по сравнению с методами ролевого и мандатного доступа. Особенно это заметно при высокой интенсивности злоумышленных атак. Так использование разработанных моделей и методов распределения доступа и защиты информации в КСКП позволяет выполнить требования гарантированного уровня безопасности в условиях, когда интенсивность $I_{атаки}$ превышает интенсивность санкционированного трафика $I_{сд}$ до 5 раз, то время когда остальные методы (мандатного и ролевого доступа) могут обеспечить данные требования только при меньших значениях интенсивностей злоумышленных воздействий. В целом следует отметить, что использование разработанных методов позволит повысить уровень безопасности информации до 1,1 раза при низкой интенсивности внешних воздействий $\left(I_{атаки}/I_{сд} \le 1\right)$, и до 1,5 раз при высокой интенсивности воздействий $\left(I_{атаки}/I_{сд} > 1\right)$.

Таким образом, исследования показали целесообразность использования разработанных моделей и методов распределения доступа и защиты информации в условиях внешних воздействий для обеспечения гарантированного уровня безопасности.

Заключение

Разработаны методические рекомендации по использованию моделей и методов распределения доступа и защиты информации в компьютерных системах критического применения, в которых выделены критерии оптимизации и способов настройки параметров и приведены примеры распределения весовых коэффициентов для типовых компонент КСКП.

Разработана имитационная модель системы распределения доступа и защиты информации в КСКП, которая позволила провести экспериментальные исследования и оценить эффективность использования разработанных моделей и методов в системе обеспечения безопасности информации. Результаты экспериментов показали, что использование предложенных моделей и методов позволит до 1,5 раз увеличить время безопасного функционирования системы.

Список литературы

1. Калинин М.О. Адаптивное управление безопасностью информационных систем на основе логического моделирования: дис. доктора техн. наук: 05.13.19 [Текст] / Калинин Максим Олегович. – СПб., 2010. – 308 с.

2. Семенов С.Г. Анализ и синтез защищенных компьютерных систем и сетей / С.Г. Семенов, А.А. Подорожняк, А.И. Баленко. – Х: НТУ«ХПИ», 2012.

3. Семенов С.Г. Модели и методы управления сетевыми ресурсами в информационно-телекоммуникационных системах / С.Г. Семенов, А.А. Смирнов, Е.В. Мелешко. – Х.:НТУ«ХПИ», 2012. – 220 с.

4. Семенов С.Г. Структурно-информационный портрет информационной системы в условиях неопределенности на примере Dos-атаки / С.Г. Семенов // Радиотехника. Тем. вып.: Информационная безопасность. – Х.:ХНУРЕ. – 2011. – №166. – С. 99-106.

5. Семенов С.Г. Методика математического моделирования защищенной ИТС на основе многослойной GERT-сети / С.Г. Семенов // Вісник НТУ «ХПІ». Зб. наук. праць. Тем. випуск: Інформатика і моделювання. – Х.:НТУ «ХПІ». – 2012. – № 62 (968). – С. 173-181.

6. Семенов С.Г. Оптимальное распределение канальных ресурсов в статистическом мультиплексоре по критерию минимального сбалансированного времени доставки информационных пакетов / С.Г. Семенов // Mat. IV НТК ХУ ПС. – Х: ХУ ПС – 2008. – С. 151.

7. Semenov S.G. The method of processing and identification of telecommunication traffic based on BDS-tests / S.G. Semenov, O.A. Smirnov, E.V. Meleshko // The book of mat. Int. Conf. «Statistical Methods of Signal and Data Processing (SMSDP-2010)». – Kiev, Ukraine, National Aviation University "NAU-Druk" Publishing House, October 2010. – P. 166-168.

Поступила в редколлегию 10.09.2012

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет им. Ю. Кондратюка, Полтава.

МЕТОДИКА НАЛАГОДЖЕННЯ ПАРАМЕТРІВ РОЗПОДІЛУ ДОСТУПУ І ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ КРИТИЧНОГО ЗАСТОСУВАННЯ

С.Г. Семенов

Представлені методичні рекомендації щодо налагодження параметрів розподілу доступу і захисту інформації в комп'ютерних системах критичного застосування (КСКЗ). Розроблена імітаційна модель системи розподілу доступу і захисту

інформації в КСКЗ. Представлена методика вибору раціонального варіанту настройки параметрів КСКЗ.. Проведена оцінка ефективності розроблених моделей і методів розподілу доступу і захисту інформації в КСКЗ. в умовах зовнішніх дій.

Ключові слова: *комп'ютерна система критичного застосування, зовнішні зловмисні дії, розподіл доступу, захист інформації.*

METHOD OF TUNING OF PARAMETERS OF DISTRIBUTING OF ACCESS AND PROTECTION IN COMPUTER SYSTEMS OF CRITICAL APPLICATION

S.G. Semenov

Methodical recommendations are presented on the use of models and methods of distributing of access and protection in the computer systems of critical application (CSCA). The simulation model of the system of distributing of access and protection is developed in CSCA. The method of choice of rational variant of tuning of parameters of CSCA is presented. The estimation of efficiency of the developed models and methods of distributing of access and protection is made in CSCA in the conditions of external influences.

Keywords: *computer system of critical application, external ill-intentioned influences, distributing of access, protection.*