УДК 681.3

РОЛЕВАЯ БЕЗОПАСНОСТЬ В DOT NET В СВЕТЕ ЭТАЛОННОЙ МОДЕЛИ ЗАЩИЩЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

А.С. Дубровин [1]
В.И. Сумин [2]

[1] Воронежская государственная технологическая академия

[2] Воронежский институт МВД России

e-mail: kiziltashman@yandex.ru

Рассматривается проблема реализации эталонной модели защищенной автоматизированной системы (ЭМЗАС) на платформе .NET. Предложен методологический подход к моделированию с использованием теоретико-графового аппарата ЭМЗАС-сетей многоуровневой авторизации в эталонной автоматизированной системе обработки данных, реализованной посредством ролевого механизма управления доступом к информации в .NET Framework.

Ключевые слова: эталонная модель защищенной автоматизированной системы (ЭМЗАС), автоматизированная система обработки данных (АСОД) критического применения (КП) .NET Framework, разрешения безопасности, разрешения принципалов, удостоверение, принципал, суперблок ЭМЗАС-сети.

Данная работа лежит в русле научных исследований по реализации математических моделей, предложенных в [6-8] на конкретных программных платформах с использованием подходящих современных информационных технологий.

Механизмом внедрения концепции эталонной автоматизированной системы обработки данных (АСОД) в смысле эталонной модели защищенной автоматизированной системы (ЭМЗАС) [5, 9] является организация расширяемой библиотеки ЭМЗАС-классов как строительного материала АСОД критического применения. АСОД критического применения появились в результате внедрения вычислительной техники в сфере критических объектов (военные объекты, экологически опасные производства, атомные станции, объекты транспорта, связи, финансово-кредитной сферы и т.д.), характеризующихся неприемлемостью для общества ущерба от нарушения их работоспособности [3]. Требования к программно-технической реализации АСОД критического применения отличаются приоритетом их надежности и защищенности от несанкционированного доступа над функциональностью.

Библиотека ЭМЗАС-классов может создаваться как независимо от существующих программных платформ, так и на базе каких-либо из них. Наиболее подходящей для этого платформой представляется Microsoft .NET (кратко – .NET) [4, 10], появление которой можно считать самой заметной революцией в программировании за последние годы. Фактически, за этой платформой будущее, поэтому особенно актуальна проблема реализации ЭМЗАС именно на ней.

Исходной предпосылкой создания платформы .NET явилась идея о том, что в глобальном информационном мире коммуникативная составляющая любых программных продуктов начинает играть определяющую роль. Платформа .NET предполагает, в частности, наличие открытых стандартов коммуникации, переход от создания монолитных приложений к созданию компонентов с легко расширяемой функциональностью, допускающих повторное использование в разных средах и приложениях. Это потребовало кардинально изменить сам принцип разработки программного обеспечения, начиная с создания нового языка и кончая созданием базиса для возможности прозрачной интеграции приложений, написанных на разных языках. Эта интеграция отлично работает с объектно-ориентированными языками, предоставляя разработчиком новый, структурированный по принципам объектно-ориентированного программирования программный интерфейс самой системы.

Основу платформы Microsoft .NET составляют четыре базовых компонента:

- .NET Building Block Services – средства программного доступа к таким службам, как хранилище файлов (file storage), календарь (calendar), служба аутентификации "Passport.NET";

- программное обеспечение для устройств .NET, которое будет выполняться на новых устройствах Интернета;

- средства .NET для работы с пользователями, включающие естественный интерфейс (natural interface), информационные агенты (information agents) и интеллектуальные теги (smart tags) – технологию, которая автоматизирует переход по гиперссылкам к информации, связанной со словами и фразами в документах пользователей;

- инфраструктура .NET, состоящая из .NET Framework, Microsoft Visual Studio.NET, .NET Enterprise Servers и Microsoft Windows.NET.

Инфраструктура .NET связана со всеми технологиями, составляющими новую среду создания и выполнения надежных, масштабируемых, распределенных приложений. Та часть .NET, с помощью которой разрабатываются такие приложения, называется единым каркасом среды разработки .NET Framework. Создание каркаса .NET Framework явилось центром обеспечиваемого платформой Microsoft .NET перехода на вычислительную модель, в которой устройства, службы и компьютеры работают совместно, обеспечивая создание решений для пользователей.

«Родной» средой для платформы .NET является открытая среда разработки программных продуктов Microsoft Visual Studio.NET, а «родным» языком, специально разработанным Microsoft для нее – C# [1, 4, 10]. Поэтому именно язык C# в среде Visual Studio фактически гарантирует наличие интерфейса практически ко всем функциональным возможностям .NET Framework. Двумя основными компонентами каркаса .NET Framework являются общеязыковая среда выполнения – Common Language Runtime (CLR) и библиотека классов каркаса – Base Class Library (BCL). Таким образом, проблема реализации ЭМЗАС на платформе .NET сводится к проблеме организации расширяемой библиотеки ЭМЗАС-классов на основе базовой библиотеки классов BCL единого каркаса среды разработки .NET Framework с использованием языка программирования C# в открытой среде разработки программных продуктов Microsoft Visual Studio.NET.

Основой каркаса .NET Framework является среда CLR. Ее можно считать агентом, который управляет кодом во время выполнения и предоставляет основные службы, такие как управление памятью, управление потоками и удаленное взаимодействие. CLR оказывается весьма удобным средством создания и поддержания в АСОД критического применения изолированной программной среды, необходимой для реализации ЭМЗАС. Такая изолированная программная среда формируется из управляемого кода, который выполняется только в среде CLR и управляем ею. Что касается непосредственной реализации политики безопасности ЭМЗАС, то для этого необходимо использовать возможности авторизации на основе ролей, поддержку которой обеспечивает среда CLR при помощи предоставляемых BCL соответствующих специальных классов.

Каркас .NET Framework предоставляет два общих механизма управления доступом к информации: управление доступом для кода и безопасность на основе ролей [2]. Они построены на основе единой согласованной модели, используют общую инфраструктуру, предоставляемую средой CLR, и их описание опирается на ряд общих основополагающих понятий. Среда CLR позволяет коду выполнять только те операции, на выполнение которых у кода есть разрешение. Она использует объекты, называемые разрешениями безопасности (Permission), для реализации механизмов, контролирующих соблюдение ограничений для управляемого кода.

Существует три вида разрешений безопасности, два из которых (разрешения доступа кода и разрешения удостоверений) относятся к управлению доступом для кода, а лишь единственный вид разрешений безопасности (разрешения принципалов) относится к безопасности на основе ролей. Разрешения принципалов (PrincipalPermission) позволяют установить, имеет ли пользователь (или действующее от его имени лицо)

конкретное удостоверение или является ли он участником указанной роли. Сам по себе методологический подход к авторизации на основе таких разрешений принципалов является достаточно общим [2]. Весь вопрос заключается в том, как интерпретировать понятия удостоверения и роли.

Сначала рассмотрим традиционную трактовку этих понятий в .NET Framework. Удостоверение (Identity) – это объект, инкапсулирующий информацию о проверяемом пользователе или сущности, в общем виде содержащий имя и тип проверки подлинности. Проверка подлинности – это процесс обнаружения и проверки удостоверения, в ходе которого изучаются учетные данные пользователя и устанавливается их подлинность в контексте некоторого центра сертификации. Сведения, полученные во время проверки подлинности, могут непосредственно использоваться в коде. Иными словами, после того как удостоверение обнаружено, можно использовать средства безопасности на основе ролей в .NET Framework для того, чтобы определить, следует ли предоставить предъявителю удостоверения доступ к коду. Именованный набор предъявителей удостоверений (участников роли), обладающих одинаковыми привилегиями в плане безопасности, называется ролью. Участвовать можно как в одной, так и в нескольких ролях. Приложения могут использовать членство в ролях для определения того, имеет ли участник роли право на выполнение запрошенного действия.

Безопасность на основе ролей в .NET Framework поддерживает авторизацию путем формирования принципала, доступного для текущего потока (текущего принципала). Принципал (Principal) – это объект, инкапсулирующий единичное удостоверение и (возможно) множественные роли, ассоциированные с пользователем. Принципал действует от имени пользователя, представляя удостоверение пользователя и его роль в качестве контекста безопасности. В ходе авторизации определяется, имеется ли для текущего принципала соответствующее разрешение принципала на выполнение запрашиваемого действия. Авторизация происходит после проверки подлинности и использует сведения об удостоверении и ролях текущего принципала, на основании которых устанавливаются текущие разрешения принципала.

Так как ролевый механизм управления доступом к информации в .NET Framework при традиционной трактовке понятий удостоверения и роли предусматривает разграничение доступа пользователей к объектам, а не разграничение доступа субъектов вышестоящего уровня (управляющих) к субъектам нижестоящего уровня (управляемых), имеющее место в ЭМЗАС, то можно констатировать отсутствие в .NET Framework механизмов непосредственной реализации политики безопасности ЭМЗАС. Однако такие механизмы могут быть созданы на основе ролевого механизма управления доступом к информации ввиду его достаточной общности и гибкости. При описании механизма непосредственной реализации политики безопасности ЭМЗАС в .NET Framework необходимо жестко разделять трактовки одних и тех же понятий в области разграничения доступа к информации для ЭМЗАС и для .NET Framework, а также необходимо установить соответствие различных понятий такого рода между ЭМЗАС и .NET Framework (см. табл. 1).

Таблица 1

Соответствие понятий ЭМЗАС и .NET Framework при описании механизма непосредственной реализации политики безопасности ЭМЗАС в .NET Framework

.NET Framework	ЭМЗАС
Удостоверение (Identity)	Верхний модуль данного блока ЭМЗАС-сети
Роль	Вариант авторизации
Принципал (Principal)	Вариант авторизации верхнего модуля данного блока ЭМЗАС-сети
Разрешение принципала (Principal Permission)	Истинное значение признака допустимости данной авторизации данного нижнего модуля данного блока ЭМЗАС-сети

Возникает новая интерпретация понятия удостоверения в результате его адаптации к ЭМЗАС. В ЭМЗАС объект-удостоверение инкапсулирует информацию об объекте-источнике проверяемого управляющего субъекта. Понятие же роли в ЭМЗАС уже

существует и не требует пересмотра. Такая интерпретация понятий удостоверения и роли в ЭМЗАС приводит к пересмотру понятий принципала и разрешения принципала в результате их адаптации к ЭМЗАС. В ЭМЗАС объект-принципал инкапсулирует информацию о проверяемом управляющем субъекте, в частности, его авторизации, а объект-разрешение принципала инкапсулирует информацию о данном управляемом субъекте.

Получается, что в ЭМЗАС от имени данного пользователя в каждый данный момент времени действует, в общем случае, не один принципал, а множество принципалов, каждый из которых относится к своему единственному уровню ЭМЗАС. Принципал может относиться к любому уровню ЭМЗАС от второго до наивысшего уровня ЭМЗАС-сети. Аналогично, любое разрешение принципала относится к своему единственному уровню ЭМЗАС из числа всех уровней ЭМЗАС-сети кроме наивысшего. Таким образом, при реализации ЭМЗАС в .NET Framework авторизация носит многоуровневый характер и осуществляется с последовательным спуском по уровням ЭМЗАС. В качестве исходной базы для ее моделирования необходимо использовать математическую модель политики безопасности подсистемы эталонной АСОД на основе ЭМЗАС-сети [7].

Структура ЭМЗАС-сети формально представляется кортежем

$$E = \langle N, K = K[I], r = r[I,\alpha], M_{вх} = M_{вх}[I,\alpha], M_{вых} = M_{вых}[I,\alpha] \rangle,$$

где N – число авторизаций в ЭМЗАС-сети, $K[I]$ – число нижних модулей в блоке с индексом I; $r[I,\alpha]$ – признак допустимости авторизации α в модуле с индексом I, показывающий, может ли в эталонной АСОД быть инициирован из соответствующего модуля процесс с данной авторизацией;

$M_{вх} = M_{вх}[I,\alpha]$, $M_{вых} = M_{вых}[I,\alpha]$ – входная и выходная функции разметки, определяющие маркировку, или состояние, входных и выходных позиций модулей в форме булевой переменной (показывают, маркирована ли данная позиция, т.е. содержит ли фишку, причем каждая позиция может содержать не более одной фишки).

При описании множества принципалов, действующих в данный момент времени в данной эталонной АСОД и запрашиваемых ими разрешений принципалов возникает задача определения для данного момента времени перечня действующих принципалов и запрашиваемых ими разрешений принципалов в подсистеме эталонной АСОД, соответствующей заданному суперблоку $B = B_{l_н \ldots l_в}(I_0)$ уровня $l_в$ с нижним уровнем $l_н$ и индексом I_0 ЭМЗАС-сети, $1 \le l_н \le l_в \le L$, где L – число уровней ЭМЗАС-сети (15-уровневой ЭМЗАС соответствует $L = 13$). Такой перечень однозначно определяется по известной маркировке заданного суперблока. Его составление целесообразно осуществлять, исходя из установления взаимно-однозначного соответствия принципалов или разрешений принципалов с некоторым подмножеством множества $P(B) = \bigcup_{l=l_н}^{l_в} P_l(B)$ разрешающих позиций суперблока B, где $P_l(B)$, $l = \overline{l_н, l_в}$ – множество разрешающих позиций уровня l суперблока B.

Каждая из позиций множества $P(B)$ относится к одному и притом единственному множеству $P_l(B)$ (эти множества взаимно не пересекаются) и к одному и притом единственному модулю. Каждый модуль u l-го уровня суперблока B может быть формально представлен следующим кортежем:

$$u = \langle I, q = q[I,\alpha], p = p[I,\alpha] \rangle \in U_l(B) \subseteq U(B),$$

где $I = I(u)$ – индекс модуля u, $U_l(B)$ – множество модулей l-го уровня суперблока B, $U(B) = \bigcup_{l=l_н}^{l_в} U_l(B)$ – множество модулей суперблока B, $q = q[I,\alpha] \in Q_l$ – функция, ставящая в соответствие индексу I модуля и номеру авторизации α ту простую позицию q из множества Q_l всех простых позиций l-го уровня ЭМЗАС-сети, которая принадлежит данному модулю, $p = p[I,\alpha] \in P_l$ – функция, ставящая в соответствие индексу I модуля и номеру авторизации α ту разрешающую позицию q из множества P_l всех разрешающих позиций l-го уровня ЭМЗАС-сети, которая принадлежит данному модулю.

Модули и блоки суперблока B идентифицируются своим индексом в ЭМЗАС-сети. Модули l-го уровня ЭМЗАС суперблока B индексируются индексами порядка $j = L - l$, $l = \overline{l_н, l_в}$, являющимися выражениями вида $i_1 . i_2 . \ldots . i_j$, представляющими собой последовательность j натуральных чисел, записанных через точку, причем $L - l_в \le j \le L - l_н$. В основе индексации лежит отнесенность модулей уровням ЭМЗАС и нумерация модулей в содержащем их блоке. Все модули данного блока делятся на верхние и нижние (относящиеся к более высокому и более низкому уровню ЭМЗАС соответственно). Любой принадлежащий суперблоку B блок с некоторым индексом I содержит единственный верхний модуль (№ 0 в блоке) и $K[I]$ нижних модулей (с номерами от 1 до $K[I]$ в блоке). Индекс блока совпадает с индексом его верхнего модуля. Индекс нижнего модуля с номером $j = \overline{1, K[I]}$ в блоке с индексом I определяется как $I . j$. Суперблок B имеет единственный верхний модуль, причем его уровень $l_в$, а индекс I_0. Этот индекс является подиндексом индекса J любого другого модуля l-го уровня суперблока B, что обозначается как $I_0 \subset J$ или $J \supset I_0$, то есть $J = I_0 . i_1 . i_2 . \ldots . i_{l - l_в}$.

Корневая маркировка суперблока

$$\left(\forall p = p[I,\alpha] \in P_{l_в}(B)\right)\left(\left(M_{вх}[I,\alpha] = 1\right) \wedge \left(M_{вых}[I,\alpha] = 0\right)\right) \wedge$$
$$\wedge \left(\forall p = p[I,\alpha] \in P(B) \setminus P_{l_в}(B)\right)\left(M_{вх}[I,\alpha] = M_{вых}[I,\alpha] = 0\right)$$

определяет ситуацию отсутствия действующих принципалов и запрашиваемых ими разрешений принципалов.

Маркировка

$$\left(\forall p = p[I,\alpha] \in \Omega_{дг}(B)\right)\left(\left(M_{вх}[I,\alpha] = 0\right) \wedge \left(M_{вых}[I,\alpha] = 1\right)\right) \wedge$$
$$\wedge \left(\forall p = p[I,\alpha] \in P(B) \setminus \Omega_{дг}(B)\right)\left(M_{вх}[I,\alpha] = M_{вых}[I,\alpha] = 0\right)$$

суперблока B ЭМЗАС-сети, индуцированная дискреционной политикой безопасности с заданными разрешающим представлением

$$\Omega_{дp}(B) = \bigcup_{l=l_н}^{l_в} \Omega_{дl}(B) \subseteq P(B)$$

и глобализованным представлением $\Omega_{дг}(B) \subseteq \Omega_{дp}(B)$, получающимся из него как

$$\left(p[I,\alpha] \in \Omega_{дг}(B)\right) \Leftrightarrow \left(\left(p[I,\alpha] \in \Omega_{дp}(B)\right) \wedge \left(\forall J \supset I \middle| p[J,\alpha] \in P(B)\right)\left(p[J,\alpha] \notin \Omega_{дp}(B)\right)\right),$$
$$\alpha = \overline{1, N},\ I = I(u),\ u \in U(B),$$

определяет перечень действующих принципалов, взаимно-однозначно соответствующих элементам множества $\Omega_{\partial p}(B)\setminus\Omega_{\partial z}(B)$, и перечень запрашиваемых ими разрешений принципалов, взаимно-однозначно соответствующих элементам множества $\Omega_{\partial p}(B)\setminus P_{l_в}(B)$.

Если глобальная политика безопасности $\Omega_z(B)$ на суперблоке B ЭМЗАС-сети, определяемая как $\Omega_z(B)\subseteq P_{l_н}(B)$,индуцирована дискреционной политикой безопасности с разрешающим представлением $\Omega_{\partial p}(B)$, то есть $\Omega_z(B)=\Omega_{\partial z}(B)$, то маркировка

$$(\forall p=p[I,\alpha]\in\Omega_z(B))\big((M_{вх}[I,\alpha]=0)\wedge(M_{вых}[I,\alpha]=1)\big)\wedge$$
$$\wedge(\forall p=p[I,\alpha]\in P(B)\setminus\Omega_z(B))(M_{вх}[I,\alpha]=M_{вых}[I,\alpha]=0)$$

суперблока B ЭМЗАС-сети, индуцированная заданной глобальной политикой безопасности $\Omega_z(B)$, определяет перечень действующих принципалов, взаимно-однозначно соответствующих элементам множества $\Omega_{\partial p}(B)\setminus\Omega_z(B)$, и перечень запрашиваемых ими разрешений принципалов, взаимно-однозначно соответствующих элементам множества $\Omega_{\partial p}(B)\setminus P_{l_в}(B)$.

Таким образом, исходя из математической модели политики безопасности подсистемы эталонной АСОД можно моделировать многоуровневую авторизацию в эталонной АСОД, реализованную посредством ролевого механизма управления доступом к информации в .NET Framework.

Литература

1. Албахари, Дж. C# 3.0. Справочник [Текст] / Дж. Албахари, Б. Албахари ; перевод с англ. – 3-е изд. – СПб. : БХВ-Петербург, 2009. – 944 с.

2. Брэгг, Р. Безопасность сетей. Полное руководство [Текст] / Р. Брэгг, М. Родс-Оусли, К. Страссберг ; перевод с англ. – М. : Издательство «ЭКОМ», 2006. – 912 с.

3. Герасименко, В.Г. Проблемы обеспечения информационной безопасности при использовании открытых информационных технологий в системах критических приложений [Текст] / В.Г. Герасименко // Информация и безопасность : региональный науч.-технический вестник. – Воронеж : Воронеж. гос. техн. ун-т, 1999. – Вып. 4. – С. 66-67.

4. Глинн, Дж. C# 2005 и платформа .NET 3.0 для профессионалов [Текст] / Дж. Глинн, Б. Ивьен, К. Нейгел, М. Скиннер, К. Уотсон ; перевод с англ. – М. : Вильямс, 2008. – 1789 с.

5. Дубровин, А.С. Информационная безопасность и защита информации в экономических информационных системах [Текст] : учеб. пособие / А.С. Дубровин, М.Г. Матвеев, Е.А. Рогозин, В.И. Сумин. – Воронеж : Воронеж. гос. технол. акад., 2005. – 292 с.

6. Дубровин, А.С. Математическая модель политики безопасности эталонной автоматизированной системы на основе ЭМЗАС-сети [Текст] / А.С. Дубровин, В.И. Сумин, М.В. Коротков, А.Ю. Немченко // Вестник ВГУ. Сер. Физика. Математика. – Воронеж : Воронеж. гос. ун-т, 2005. – № 2. – С. 147-155.

7. Дубровин, А.С. Математическая модель политики информационной безопасности подсистемы эталонной автоматизированной системы обработки данных на основе ЭМЗАС-сети [Текст] / А.С. Дубровин, В.И. Сумин // Научные ведомости Белгород. гос. ун-та. Сер. История Политология Экономика Информатика. – 2009. – № 1 (56). – Вып. 9/1. – С. 26-44.

8. Дубровин, А.С. Слоистая структура ЭМЗАС-сети [Текст] / А.С. Дубровин, В.И. Сумин, С.В. Родин, Г.В. Перминов // Вестник Воронежского института МВД России. – Воронеж : Воронеж. ин-т МВД России, 2007. – № 1. – С. 153-158.

9. Сумин, В.И. Эталонная модель защищенной автоматизированной системы [Текст] / В.И. Сумин, А.С. Дубровин // Материалы международной науч.-практической конф. «Информационно-аналитическое обеспечение раскрытия и расследования преступлений правоохранительными органами», 24–25 мая 2007 г. – Белгород: Белгород. юр. ин-т МВД России, 2007. – С. 52-58.

10. Троелсен, Э.C# и платформа .NET 3.0 [Текст] / Э. Троелсен ; перевод с англ. – Спец. изд. – СПб. : Питер, 2008. – 1456 с.

ROLE SAFETY IN DOT NET IN THE LIGHT OF THE PROTECTED SYSTEM STANDARD MODEL

A.S. Dubrovin [1]
V.I. Sumin [2]

[1] *Voronezh State Technological Academy*

[2] *Voronezh Institute of the Ministry of Internal Affairs of Russia*

e-mail: kiziltashman@yandex.ru

The problem of the protected system standard model (PSSM) implementation on a platform .NET is considered. The methodological approach to modeling the multi-level authorization in the standard data processing system implemented by means of a role access control mechanism to the information in a .net Framework with usage the graph theory apparatus of PSSM-networks is offered.

Key words: protected system standard model (PSSM), critical application data processing system (DPS), .NET Framework, Permission, PrincipalPermission, Identity, Principal, superblock of the PSSM-networks.