Утрачиваемое искусство доказательства защищенности. Часть 1 из 2

Пашков Юрий, Пашков Кузьма

Многолетний опыт преподавания по направлению «Информационная безопасность» (далее ИБ) позволяет констатировать положительные тенденции в этой области:

- Владельцы бизнеса, наконец, стали считать риски ИБ такими же значимыми как финансовые и операционные, и все чаще ищут не только доверенных, но квалифицированных советников на должности уровня CSO (Chief Security Officer)
- Нормативный подход к построению систем защиты позволил ИБ стать массово потребляемой услугой
- Взрывной рост рисков ИБ поддерживает стабильно высокий спрос и предложение на рынке услуг обучения по соответствующему направлению

В тоже время налицо и отрицательные:

- Подтвердить свою квалификацию в ИБ сегодня так же сложно, в особенности если успешный опыт работы получен в странах СНГ, а потенциальный работодатель находится в США\Европе
- Массовость приводит к проблеме консьюмеризации ИБ
- Падает качество услуг обучения и уровень квалификации специалистов

В результате появляются целые коллективы подразделений обеспечения ИБ, которые на всех уровнях иерархии, начиная с администратора безопасности и заканчивая руководителем, бездумно выполняют требования стандартов безопасности, не задумываясь о доказательстве защищенности автоматизированной системы после их выполнения.

Настоящая статья демонстрирует возможности доказательного подхода для создания защищенных автоматизированных систем и носит учебный характер.

1. Технология работы с данными

Предположим, что в некоторой организации используется следующая технология работы:

1) В организации сотрудники работают в составе нескольких разных отделов, решающих взаимосвязанные, но разные задачи;

2) решение задач каждого отдела автоматизировано; для решения задач отдела используется общая база данных, доступная всем сотрудникам отдела в рамках коллективной работы. Содержание базы данных тайной не является, однако ее доступность является критическим параметром для деятельности отдела и организации в целом. Иначе говоря, если база данных не будет доступна, то организация понесет ущерб;

3) при выполнении сотрудниками служебных обязанностей используются конфиденциальные сведения, содержащиеся в документах. Иначе говоря, если содержание документов станет известно неограниченному кругу лиц, то организации может быть нанесен ущерб;

4) документы разрабатываются и печатаются сотрудниками с помощью средств автоматизации на своих автоматизированных рабочих местах (далее – АРМ), подключенных к локальной вычислительной сети (далее – ЛВС).

Для создания документов используются средства многозадачной операционной системы. Операционная система (далее – ОС) позволяет пользователю запустить на выполнение несколько программ. Данные документов хранятся в файлах и обрабатываются программами ОС.

Коллективная работа обеспечивается с помощью АРМ сотрудников, сетевого оборудования ЛВС, сервера и средств сетевой операционной системы.

2. Политика безопасности

Рассмотрим избирательную политику безопасности, которая может быть использована в нашем случае:

1) документы и БД организации являются ценными. Должна быть реализована система разграничения доступа к документам и БД на основе комплекса организационно-технических мер и средств защиты;

2) система автоматизации замкнутая — к документам и БД имеют доступ только должностные лица организации;

3) управление организации в лице администратора системы имеет право доступа ко всем документам и БД;

4) руководитель организации с помощью администратора определяет права по доступу сотрудников к документам и БД;

5) сотрудники имеют право доступа к объектам, созданным ими самими, а также являющимся объектом коллективного использования группы пользователей, к которой данный сотрудник принадлежит;

6) доступ от имени некоторого пользователя к объектам, созданным другим пользователем или принадлежащим объектам коллективного использования группы пользователей, к которой данный пользователь не принадлежит, запрещен.

Политика безопасности и механизмы поддержки ее реализации образуют единую защищенную среду обработки информации. Эта среда имеет иерархическую архитектуру, где верхние уровни представлены требованиями политики безопасности, далее следует интерфейс пользователя, затем идут несколько программных уровней защиты (включая уровни ОС) и, наконец, нижний уровень этой структуры представлен аппаратными средствами защиты. На всех уровнях, кроме верхнего, должны реализовываться требования политики безопасности, за что, собственно, и отвечают механизмы защиты.

В различных системах механизмы защиты могут быть реализованы по-разному; их конструкция определяется общей концепцией системы. Однако одно требование должно выполняться неукоснительно: эти механизмы должны адекватно реализовывать требования политики безопасности.

Для примера рассмотрим, как может быть реализована эта политика безопасности при использовании модели нашей автоматизированной системы.

3. Модель автоматизированной системы

Построим модель автоматизированной системы, оперирующей ценной информацией. Ценная информация хранится в системе в виде информационных объектов. Кроме ценной информации объекты могут содержать другую информацию, например, тексты программ, служебную информацию системы и т.п.

Пусть время дискретно и принимает значения из N — множества значений времени, $N = (1,2, \dots)$. Обозначим через $t \in N$ текущее значение времени.

Принято считать, что состояние системы в данный момент может быть представлено в виде состояний конечного множества объектов. Поэтому будем считать, что состояние системы — это набор состояний ее объектов. Объекты могут создаваться и уничтожаться, поэтому можно говорить о множестве объектов системы в некоторый момент времени $t \in N$, которое определим как O_t, $|O_t| < \infty$ — множество объектов системы в момент времени t. Множество объектов конечно. Под объектом будем понимать произвольное конечное множество слов некоторого языка Я.

Для каждого $t \in N$ из множества O_t объектов системы выделим некоторое подмножество S_t,— множество субъектов системы в момент времени t. Множество S_t состоит из субъектов системы *S.* Под субъектом будем понимать объект, описывающий преобразование, которому выделен домен (под доменом понимаются ресурсы системы, выделенные для преобразования) и передано управление. Преобразование, которому передано управление, называется процессом. Таким образом, субъект— это пара (домен, процесс). Каждый субъект может находиться в двух состояниях: в форме

описания, в котором он называется неактивизированным, и в форме (домен, процесс), в которой он называется активизированным.

Активизировать субъект может только другой активизированный субъект. На множестве *S*, субъектов системы для каждого момента времени $t \in N$ определим граф Γ_t , — граф функционирования системы. Вершины S_1 и S_2 графа соединены дугой $S_1 \to S_2$ тогда и только тогда, когда в случае активизации S_1 возможна активизация S_2. Если в любой момент времени $t \in N$ в графе Γ_t, в вершину *S* не входят дуги и не выходят дуги, то такие субъекты исключим из рассмотрения. Обозначим через $S_1 \overset{a}{\to} S_2$ процедуру активизации субъекта S_2 субъектом S_1. Под активизацией будем понимать передачу управления субъектом S_2 субъекту S_1.

Из множества S_t субъектов системы выделим подмножество *U* — множество пользователей системы. Под пользователем понимается такой субъект *S* из множества субъектов, для которого во всех графах Γ_t, в вершину *S* не входят дуги. Пользователи активизированы по определению и могут активизировать другие субъекты системы. Введем понятие группы пользователей, которую будем обозначать как G. Под группой пользователей понимается подмножество множества пользователей U, в которое включены пользователи, имеющие равные права по доступу к объектам коллективного использования группы. Кроме активизации в системе возможны и другие виды доступов. Определим множество R — множество видов доступа. Множество конечно, т.е. $|R| < \infty$. Примерами видов доступа являются «чтение», «запись», «исполнение». Для каждого субъекта *S* можно определить ρ — множество доступов активизированного субъекта *S* к объекту *O*, которое является подмножеством множества видов доступа $\rho \subseteq R$.

Обозначим $S \to O$ —доступ субъекта *S* к объекту *O*. Непосредственный доступ субъекта *S* системы к объекту *O* системы не всегда возможен. Определим тогда $S \to* O$ — доступ от имени субъекта *S* к объекту *O*. Это означает, что в некоторый промежуток времени $[t, t+\tau]$ реализована последовательность доступов

$$S \overset{a}{\to} S_1 \overset{a}{\to} S_2 \overset{a}{\to} \dots \overset{a}{\to} S_k \overset{\rho}{\to} O$$

Поскольку функционирование системы описывается доступами активизированных субъектов системы к объектам системы, то для каждого момента времени $t \in N$ можно определить

$$D_t = \{O|\text{S}\to*\text{O в момент времени t}\}$$

— множество объектов, к которым осуществляется доступ в момент времени $t \in N$.

В этом множестве выделим

$$D_t(U) = \{O|\text{U}\to*\text{O в момент времени t}\}$$

— множество объектов, к которым осуществляется доступ от имени пользователя *U* в момент времени $t \in N$, а также

$$D_t(G) = \{O|U_i\to*\text{O}, U_i \in \text{G, i=1(1)n в момент времени t}\}$$

— множество объектов, к которым осуществляется доступ группой пользователей в момент времени $t \in N$.

Из множества объектов, к которым возможен доступ, выделим группу объектов, к которым осуществляется обращение всех пользователей

$$D = \bigcap_t D_t(U_i), i = 1(1)n$$

Это общие объекты системы. В частности, средствами из D пользователь может создавать объекты и уничтожать объекты, не принадлежащие D. Для каждой группы пользователей можно выделить также множество объектов

$$D_g(G) = \bigcap_t D_t(G)$$

— объекты коллективного использования группы *G*.

Будем считать, что из объектов системы построена некоторая подсистема, которая реализует доступы. Будем полагать, что любое обращение субъекта за доступом к объекту в эту подсистему начинается с запроса, который будем обозначать $S \overset{\rho?}{\to} O$.

При порождении объекта субъект, активизированный от имени пользователя, обращается к соответствующей процедуре, в результате которой создается объект с уникальным именем. Будем считать, что соответствующий пользователь породил

данный объект. Обозначим через $O_t(U)$— множество объектов, порожденных пользователем. Аналогичным образом можно определить и $O_t(G)$ — множество объектов, порожденных группой пользователей.

Среди всех пользователей выделим привилегированного пользователя $\mathrm{U_{adm}}$ — администратора системы. Данный пользователь имеет полный набор привилегий по доступу к общим объектам системы. В любой момент времени $t \in N$ этот пользователь единственен.

Теперь выразим в терминах модели политику безопасности, определяющую разрешенные и неразрешенные доступы в системе.

Разрешенными будем считать доступы к объектам, созданным самим пользователем, а также принадлежащие объектам коллективного использования группы пользователей, к которой данный пользователь принадлежит. Математически это можно сформулировать следующим образом:

если $S \overset{\rho?}{\to} O$, то при $U \overset{a}{\to} * S, O \in O_t(U)$ или $U \overset{a}{\to} * S, O \in D_g(G), U \in G$, то доступ $S \overset{\rho}{\to} O$ разрешен.

Будем считать неразрешенными доступы от имени некоторого пользователя к объектам, созданным другим пользователем, или принадлежащие объектам коллективного использования группы пользователей, к которой данный пользователь не принадлежит.

Если $U_i \overset{a}{\to} * S, O \in O_t(U_j), i \neq j$ или $U \overset{a}{\to} * S, O \in D_g(G), U \notin G$, то доступ $S \overset{\rho}{\to} O$ запрещен [1].

4. Доказательство необходимости условий безопасности

Итак, мы построили модель системы, ведущей обработку ценной информации, и сформулировали высказывания, справедливость которых в общем случае представляется спорной.

Теперь необходимо доказать, что при выполнении определенных условий эти высказывания будут истинными, иначе говоря, политика безопасности будет выполняться, модель системы будет защищена и вести обработку информации в системе будет безопасно.

Сначала мы интуитивно введем ряд предположений, обеспечивающих, по нашему мнению, безопасность обработки информации. Далее мы докажем, что выполнение этих предположений обеспечит выполнение политики безопасности. От предположений мы перейдем к «услугам» более низкого уровня, выдвинем условия, при которых модель системы будет защищена, а также докажем этот факт.

Таким образом, доказав защищенность модели, мы можем говорить, что построенная нами модель системы является защищенной. После проведенных доказательств можно утверждать, что если модель системы защищена, то и система, реализованная в точном соответствии с условиями, сформулированными при моделировании, тоже будет защищена.

Предположение 1. Если субъект *S* активизирован в момент t, то существует единственный активизированный субъект *S'* в S_t, который активизировал *S*. В момент *t* = 0 активизированы только пользователи.

Лемма 1. Если в данный момент *t* активизирован субъект *S,* то существует единственный пользователь *U,* от имени которого активизирован субъект *S,* т. е. существует цепочка

$$U \overset{a}{\to} S_1 \overset{a}{\to} S_2 \overset{a}{\to} \ldots \overset{a}{\to} S_k \overset{\rho}{\to} O$$

Доказательство. Согласно предположению 1 существует единственный субъект S_k, активизирующий *S.* Если $S_k = U_i, \mathrm{U_i} \in \{\mathrm{U}\}$, то лемма доказана.

Если $S_k \neq U_i$, то существует единственный субъект S*k*-1 > активизировавший *Sk.* В силу конечности времени работы системы Σ и того факта, что в начальный момент времени активизированы могут быть только пользователи, находим в начале цепочки одного из них. На этом, согласно определению пользователей, цепочка обрывается.

Лемма доказана.

Будем моделировать функционирование системы последовательностью доступов активизированных субъектов системы к объектам системы.

Предположение 2. Функционирование системы Σ описывается последовательностью доступов множеств субъектов к множествам объектов в каждый момент времени $t \in N$.

Л е м м а 2. Для каждого $t \in N$, для каждого $O \in O_t, O \notin D$ существует единственный пользователь *U*, такой что $O \in O_t(U)$, т. е. его породивший.

Доказательство. Поскольку $O_0 = \{U_i\} \cup D$ то объект $O \in O_t, O \notin D$ порожден в некоторый момент s,$0 \le s \le t$. Тогда в O_s существовал активизированный субъект *S*, создавший *O*. Тогда, как отмечено ранее, существует единственный пользователь *U*, породивший *O*. Лемма доказана.

Одним из недостатков дискреционной политики безопасности является свободное распространение прав. Предположим, что только один пользователь в системе имеет все права по доступу к общим объектам системы, являясь, таким образом, их владельцем, и права эти в полном объеме он никому не передает.

Предположение 3. В системе Σ в каждый момент времени $t \in N$ существует единственный пользователь U_{adm}, который обладает всеми правами по отношению к общим объектам системы.

Предположим, что невозможно сохранить какую-либо ценную информацию в объектах общего доступа.

Предположение 4. Если O ∈ D, то доступы вида $U_i \overset{\rho_1}{\to} * O, U_j \overset{\rho_2}{\to} * O, i \neq j$, при любых $\rho_1, \rho_2 \subseteq R$ не могут создать канал утечки информации.

Предположим, что порядок работы системы при попытке обращения субъекта, активизированного от имени некоторого пользователя к объекту системы, следующий.

Предположение 5. Если некоторый субъект $S, S \in D$ активизирован от имени пользователя U_i (т. е. $U_i \overset{a}{\to} * S$), в свою очередь субъекту *S* предоставлен в момент *t* доступ к объекту *O*, то либо $O \in D$, либо $O \in O_t(U_i)$, либо $O \in D_g(G)$, $U_i \in G$, либо система аварийно прекращает доступ.

Теорема 1. Пусть в построенной системе выполняются предположения 1-5 и правила политики безопасности. Тогда в системе несанкционированный доступ невозможен.

Доказательство. Предположим противное, т. е. что существует в некий момент времени t такой вид доступа *p*, при котором от имени пользователя U_i не входящего в группу, осуществляется доступ к объекту *O* другого пользователя U_j или к общим объектам другой группы:

$$\exists t, \exists \rho \subseteq R, \rho \neq \emptyset, \exists U_i, U_i \notin G, \exists O \in O_t, U_i \overset{\rho}{\to} * O$$

при $\begin{cases} O \in O_t(U_j), i \neq j, \\ O \in D_g(G), U_i \notin G. \end{cases}$

Пусть $S_1, S_2, \ldots, S_m$ – все активизированные субъекты, имеющие доступы $\beta_i \subseteq \rho, i = 1,2,\ldots,m$ в момент времени t к объекту O. Тогда, согласно лемме 2, множество этих субъектов разбивается на три подмножества:

Общие объекты:

$$A = \{S_l | S_l \in D\};$$

Субъекты, являющиеся объектами, порожденными от имени пользователя U_i или от группы G:

$$B = \{S_l | S_l \in O_t(U_i), S_l \in D_t(G), U_i \in G\};$$

Субъекты, являющиеся объектами, осуществляющие несанкционированный доступ (по предположению):

$$C = \{S_l | S_l \in O_t(U_j), i \neq j, S_l \in D_t(G), U_i \notin G\}.$$

Согласно лемме 1, для любого S_l, l=1,2,…,m, существует единственный пользователь, от имени которого активизирован субъект S_l. Если $S_l \in A$, то, согласно предположению 5 и условию теоремы 1, что доступ $S_l \overset{\beta_l}{\to} * O$ разрешен, получаем, что S_l

активизирован от имени U_j или $U_i \in G$. Это противоречит предположению.

Если $S_l \in B$, то доступ $S_l \overset{\beta_l}{\to} * O$ невозможен согласно политике безопасности.

Значит, если $U_i \overset{\rho}{\to} * O$, то существует цепочка длины (k+1):

$$U_i \overset{\rho_1}{\to} S^{(1)} \overset{\rho_2}{\to} S^{(2)} \overset{\rho_3}{\to} \dots \overset{\rho_k}{\to} S^{(k)} \overset{\rho}{\to} O$$

и субъект $S^{(k)} \in C$.

Тогда существует цепочка длины k, такая что

$$U_i \overset{\propto}{\to} * O', O' \in O_{t-1}(U_j), i \neq j, O' \in D_{t-1}(G), U_i \notin G, \propto \subseteq R.$$

Повторяя эти рассуждения, через k шагов получим, что

$$U_i \overset{\propto}{\to} * O'', O'' \in O_{t-k}(U_j), i \neq j, O'' \in D_{t-k}(G), U_i \notin G, \beta \subseteq R.$$

Последний доступ невозможен, если выполняется политика безопасности. Поэтому предположение неверно и теорема 1 доказана.

Теперь построим более удобное для реализации в автоматизированной системе множество «услуг» более низкого уровня, поддерживающих политику безопасности, т.е. мы хотим определить множество условий, реализованных в системе, таких, что можно доказать теорему о достаточности выполнения правил политики безопасности.

Условие 1 (*идентификация и аутентификация*). Если для любых $t \in N$, $\rho \subseteq R$, $O \in O_t$, $S \overset{\rho?}{\to} O$, то вычислены функции принадлежности *S* и *O* к множествам $O_t(U_i), i = 1(1)n$; $D; D_g(G_k), k = 1(1)g$.

Условие 2 (*разрешительная подсистема*). Если $U_i \overset{\propto}{\to} * S, O \in O_t(U_j)$ и $S \overset{\rho?}{\to} O$ в момент t, то из $t = j$ следует $S \overset{\rho}{\to} O$ и из $t \neq j$ следует $S \overset{\rho|}{\to} O$. Аналогично, если U$\overset{\propto}{\to} * S, O \in D_g(G)$ и $S \overset{\rho?}{\to} O$ в момент t, то из $U \in G$ следует $S \overset{\rho}{\to} O$ и из $U \notin G$ следует $S \overset{\rho|}{\to} O$.

Условие 3 *(отсутствие обходных путей)*. Для любых $t \in N$, $\rho \subseteq R$, если субъект *S*, активизированный к моменту *t*, получил в момент *t* доступ $S \overset{\rho}{\to} O$, то в момент *t* произошел запрос на доступ $S \overset{\rho?}{\to} O$.

Т е о р е м а 2. Если в построенной системе выполняются условия 1-3, то выполняется политика безопасности (достаточность условий для выполнения политики).

Доказательство. Утверждение теоремы состоит из двух утверждений:

а) если для произвольного $\rho \subseteq R$, $S \overset{\rho?}{\to} O$

$$\begin{cases} U \overset{\propto}{\to} * S, O \in O_t(U), \\ U \overset{\propto}{\to} * S, U \in G, O \in D_g(G), \end{cases}$$

то доступ $S \overset{\rho}{\to} O$ разрешен;

б) если для произвольного $\rho \subseteq R$, $S \overset{\rho?}{\to} O$

$$\begin{cases} U \overset{\propto}{\to} S, O \in O_t(U_j), i \neq j, \\ U \overset{\propto}{\to} S, U \notin G, O \in D_g(G), \end{cases}$$

то какой-либо доступ в момент t субъекта S к объекту O невозможен.

Докажем утверждение а). Если $S \overset{\rho?}{\to} O$, то по условию 1 вычислены функции принадлежности и определена принадлежность субъекта *S* и объекта *O* к множествам $O_t(U_i), i = 1(1)n$; $D; D_g(G_k), k = 1(1)g$. Если $U_i \overset{\propto}{\to} * S, O \in O_t(U_j)$ и $i = j$, то выполняется посылка условия 2, и доступ разрешен. Если объект $O \in D_g(G)$, т. е. является объектом коллективного использования группы пользователей, а также пользователь $U \in G$ — член этой группы, то, согласно условию 2, пользователь также разрешен.

Докажем теперь утверждение б). Если $S \overset{\rho?}{\to} O$, вычислены функции принадлежности и определено, что $U_i \overset{\propto}{\to} * S, O \in O_t(U_j)$ и $i \neq j$, то по условию 2 доступ $S \overset{\rho}{\to} O$ не разрешен. Аналогично, если определено, что $U \overset{\propto}{\to} * S, U \notin G, O \in D_g(G)$, то доступ не разрешен, согласно посылке условия 2.

Если доступ $S \xrightarrow{\rho} O$ стал возможен, минуя запрос $S \xrightarrow{\rho?} O$ и субъект S активизирован к моменту t, то сделанное предположение противоречит условию 3. Если субъект S не активизирован, то наличие доступа $S \xrightarrow{\rho} O$ противоречит определению доступа. Теорема доказана.

Следствием теоремы 2 является тот факт, что, обеспечив выполнение условий 1-3 при функционировании системы, мы гарантируем выполнение политики безопасности.

Таким образом, если верны предположения 1-5 и при функционировании системы выполняются условия 1-3, то несанкционированный доступ к объектам системы невозможен.

Поскольку как предположения, так и условия формулировались в отношении модели автоматизированной системы, то в реальной системе должны быть реализованы механизмы, обеспечивающие их безусловное выполнение.