ВОПРОСЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. КОМПЛЕКСНЫЙ ПОДХОД К ПОСТРОЕНИЮ СРЕДСТВА ЗАЩИТЫ

А. Ю. Щеглов, *д.т.н., профессор,*
К. А. Щеглов, *ЗАО «НПП «Информационные технологии в бизнесе»*

Современная динамика развития средств защиты компьютерной информации настораживает тем, что рынок немедленно реагирует на проявление актуальности отдельных проблем появлением, как правило, целого набора специализированных средств защиты, предназначенных для решения конкретной технической задачи. Существуют специализированные средства антивирусной защиты, защиты от несанкционированного доступа (НСД), противодействия шпионским программам и т.д. Сейчас наиболее востребованной (как говорится, на слуху) является задача противодействия внутренним ИТ-угрозам. Заметим, что эта задача не нова, другое дело, что защита современных универсальных системных средств базируется на принципе полного доверия к пользователю, как следствие, именно санкционированный пользователь (а не сторонний сотрудник, либо вообще внешнее по отношению к предприятию лицо) и несет в себе наиболее вероятную угрозу хищения данных (подобных злоумышленников называют инсайдерами).

Вместе с тем, следует понимать, что всю совокупность ИТ-угроз можно разделить на внешние и внутренние (других просто априори быть не может). Как следствие, можно предположить, что эффективное средство защиты компьютерной информации должно решать задачи защиты в комплексе, обеспечивая противодействие как внешним, так и внутренним ИТ-угрозам. В противном случае применение средства защиты будет во многом просто бесполезным. Возникает вопрос, что же собою представляет комплексный подход к решению задачи защиты компьютерной информации. Возможно, набор специализированных средств защиты, решающих различные задачи, устанавливаемых на одном компьютере, позволит эффективно решить всю совокупность задач защиты в комплексе, или это должно быть средство защиты, которое должно базироваться на иных принципах построения? А в этом случае невольно, возникает вопрос: к чему приведет комплексирование различных специализированных средств?

Чтобы ответить на все эти вопросы, рассмотрим в данной работе альтернативные (в части решения задач противодействия внешним и внутренним ИТ-угрозам) подходы к реализации лишь одного механизма защиты – механизма полномочного контроля доступа к ресурсам (пойдем в своих рассуждениях от частного к общему). Этот механизм защиты для проведения исследования нами выбран не случайно. Во-первых, как увидим в работе, он наиболее показателен для наших исследований, во-вторых, на его, в том или ином виде, применении базируются известные нам средства противодействия внутренним ИТ-угрозам, в-третьих, данный механизм реализован практически во всех современных средствах защиты информации (СЗИ) от НСД, т.к. применение данного механизма защиты в качестве основного регламентируется соответствующими нормативными документами в области защиты информации, начиная с СВТ 4 класса защищенности (где он позиционируется как мандатный принцип контроля доступа).

ПОНЯТИЕ ПОЛНОМОЧНОГО КОНТРОЛЯ ДОСТУПА К РЕСУРСАМ

Ключевым механизмом защиты информации является контроль доступа к ресурсам, основанный на задании и реализации правил разграничения доступа к ресурсам для пользователей. Задаваемые правила доступа всегда могут быть представлены соответствующей моделью (или матрицей доступа).

Пусть множества C = {C1,…, Ck} и O = {O1,…, Ok} – соответственно линейно упорядоченные множества субъектов и объектов доступа. В качестве субъекта доступа Ci, i = 1,…,k рассматривается как отдельный субъект, так и группа субъектов, обладающих одинаковыми правами доступа (заметим, что на практике это могут быть как различные пользователи, так и один и тот же пользователь, обладающий различными правами доступа при различных режимах обработки информации), соответственно, в качестве объекта доступа Oi, i = 1,…,k может также рассматриваться как отдельный объект, так и группа объектов, характеризуемых одинаковыми к ним правами доступа. Пусть S = {0,Чт,Зп} – множество прав доступа, где «0» обозначает отсутствие доступа субъекта к объекту, «Чт» – разрешение доступа для чтения объекта, «Зп» – разрешение доступа для записи в объект.

Каноническую модель контроля доступа (модель контроля доступа, реализующая базовые требования к механизму защиты) можно представить матрицей доступа D, имеющей следующий вид:

$$D = \begin{array}{c} \\ O1 \\ O2 \\ \\ \\ Ok\text{-}1 \\ Ok \end{array} \begin{array}{c} \begin{array}{cccc} C1 & C2 & \ldots\ldots & Ck\text{-}1 \end{array} \quad Ck \\ \left[\begin{array}{cccc} Зп/Чт & 0 & 0 & 0 \\ 0 & Зп/Чт & 0 & 0 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0 & 0 & Зп/Чт & 0 \\ 0 & 0 & 0 & Зп/Чт \end{array}\right. \end{array}$$

Под канонической моделью контроля доступа для линейно упорядоченных множеств субъектов (групп субъектов) и объектов (групп объектов) доступа понимается модель, описываемая матрицей доступа, элементы главной диагонали которой «Зп/Чт» задают право полного доступа субъектов к объектам, остальные элементы «0» задают запрет доступа субъектов к объектам.

Заметим, что каноническая модель контроля доступа описывает режим изолированной обработки информации, при котором объекты не могут служить каналами взаимодействия информацией субъектов (пользователей).

Один из широко сегодня используемых на практике способов назначения (формализации отношения) каналов взаимодействия субъектов является полномочный контроль доступа. Широкое его практическое использование обусловлено тем, что в корпоративных приложениях, как правило, на одном и том же компьютере обрабатывается различная по уровню конфиденциальности информация, что позволяет ее категорировать («открытая», «конфиденциальная», «строго конфиденциальная», «секретная» и т.д.). При этом необходимо обеспечить различные режимы обработки информации различных категорий на основе задания соответствующих полномочий субъектам доступа (откуда и название) к категорированным объектам.

Основу полномочного контроля доступа составляет способ формализации понятий «группа» пользователей и «группа» объектов на основании вводимой шкалы полномочий. Наиболее широко на практике используется способ иерархической формализации отношения полномочий, состоящий в следующем. Иерархическая шкала полномочий вводится на основе категорирования данных (открытые, конфиденциальные, строго конфиденциальные и т.д.) и прав допуска к данным пользователей (по аналогии с понятием «формы допуска»). Будем считать, что чем выше полномочия субъекта и категория объекта, тем, соответственно, меньше их порядковый номер в линейно полномочно упорядоченных множествах субъектов и объектов – C = {C1,…, Ck} и O = {O1,…, Ok}). Соответствующая формализация правил доступа субъектов к объектам при этом, как правило, сводится к следующему:

- субъект имеет право доступа «Зп/Чт» к объекту в том случае, если полномочия субъекта и категория объекта совпадают;
- субъект имеет право доступа «Чт» к объекту в том случае, если полномочия субъекта выше, чем категория объекта;
- субъект не имеет прав доступа к объекту в том случае, если полномочия субъекта ниже, чем категория объекта.

Матрица доступа D, описывающая полномочную модель контроля доступа, имеет следующий вид.

$$D = \begin{array}{c} \\ O1 \\ O2 \\ \\ \\ Ok\text{-}1 \\ Ok \end{array} \begin{array}{c} \begin{array}{cccc} C1 & C2 & \ldots\ldots & Ck\text{-}1 \end{array} \quad Ck \\ \left[\begin{array}{cccc} Зп/Чт & 0 & 0 & 0 \\ Чт & Зп/Чт & 0 & 0 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ Чт & Чт & Зп/Чт & 0 \\ Чт & Чт & Чт & Зп/Чт \end{array}\right. \end{array}$$

Таким образом, видим, что основная задача, решаемая при реализации данного способа контроля доступа, состоит в предотвращении возможности понижения категории информации при ее обработке. Это необходимо, т.к. информация соответствующих категорий предполагает и соответствующие режимы ее обработки (возможность сохранения на мобильные накопители, печати, передачи по сети и т.д.). Естественно, что чем категория выше, тем эти режимы жестче. Все эти действия направлены на предотвращение возможности хищения конфиденциальной информации из корпоративной сети предприятия в предположении, что на вычислительных средствах может обрабатываться как открытая, так и конфиденциальная и секретная информация.

Иногда дополнительно вводится правило, разрешающее запись информации более низкой категории в объекты более высокой категории, что также не противоречит идеи противодействия понижению категории информации. Матрица доступа D, описывающая полномочную модель контроля доступа при этом, имеет следующий вид.

$$D = \begin{array}{c} \\ O1 \\ O2 \\ \\ \\ Ok\text{-}1 \\ Ok \end{array} \begin{array}{c} \begin{array}{cccc} C1 & C2 & \ldots\ldots & Ck\text{-}1 \end{array} \quad Ck \\ \left[\begin{array}{cccc} Зп/Чт & Зп & Зп & Зп \\ Чт & Зп/Чт & Зп & Зп \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ Чт & Чт & Зп/Чт & Зп \\ Чт & Чт & Чт & Зп/Чт \end{array}\right. \end{array}$$

В порядке замечания отметим, что возможность работы одного и того же пользователя с данными различных категорий рядом известных нам способов реализаций полномочного контроля доступа обеспечивается тем, что в системе реализуются динамические полномочия пользователя, изменяемые применительно к тому, с документом какой категории пользователь работает. Корректность реализации полномочного контроля здесь обеспечивается тем, что разрешается изменять категорию лишь в сторону ее повышения (Ck → Ck-1 → ……→C1) – после чтения открытого

документа пользователю разрешается сохранять данные в объект категории «открыто», после чтения конфиденциального документа пользователю разрешается сохранять данные в объект категории «конфиденциально», причем все открытые ранее документы категории «открыто» также разрешается сохранять только в объект категории «конфиденциально».

Не будем в этой работе детально останавливаться на анализе данного частного решения (это вопрос самостоятельного исследования). Однако отметим два его недостатка, сразу бросающихся в глаза, обусловленных тем, что обработка информации различных категорий при этом осуществляется под одной учетной записью. Во-первых, это приводит к тому, что информация различных категорий обрабатывается с одними и теми же привилегиями пользователя (т.е. нивелируется одно из важнейших свойств защиты современных ОС – назначение различных привилегий пользователя при обработке различных типов информации). Во-вторых, вся защита современных ОС строится на разграничениях между учетными записями. Как следствие, здесь возникает проблема, связанная с необходимостью блокировать каналы межпроцессного обмена (что ОС реализует только для различных учетных записей), а таких каналов десятки – это не только буфер обмена, но и поименованные каналы, сектора памяти и т.д. и т.п.

ПОНЯТИЕ МАНДАТНОГО ПРИНЦИПА КОНТРОЛЯ ДОСТУПА

В части реализации модели полномочного контроля доступа (реализуется диспетчером доступа, осуществляющим анализ запроса доступа субъекта к объекту, с целью принятия решения о предоставлении права на запрашиваемый доступ, если он санкционирован соответствующей моделью) могут рассматриваться следующие альтернативные варианты: контроль доступа на основании анализа матрицы доступа и контроль доступа с использованием меток безопасности (или мандатов).

Матрица доступа является отображением соответствующей модели, в данном случае полномочного контроля доступа D. При запросе доступа (по его параметрам – какой субъект к какому объекту обращается и какой доступ при этом запрашивается) диспетчером выбирается и анализируется соответствующее разрешение (элемент Dij матрицы). Если запрашиваемый доступ не противоречит заданному разрешению, он признается диспетчером санкционированным – запрашиваемый доступ субъекта к объекту разрешается.

Применение механизма меток безопасности (мандатов) – это уже попытка формализации назначения и анализа прав диспетчером доступа (т.е. это способ обработки запроса диспетчером доступа). Вот какие требования (выдержка) к реализации мандатного принципа контроля доступа формулируются в соответствующем нормативном документе:

«КСЗ (комплекс средств защиты) должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и иерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;
- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта».

В части вопросов технической реализации это означает следующее. Метки безопасности (еще называют мандатами) являются элементами линейно упорядоченного множества M = {M1,…, Mk}. Метки безопасности назначаются субъектам и объектам (группам субъектов и объектов), служат для формализованного представления их уровня полномочий. Будем считать, что чем выше полномочия субъекта и категория объекта (меньше их порядковый номер в линейно полномочно упорядоченных множествах субъектов и объектов – C = {C1,…, Ck} и O = {O1,…, Ok}), тем меньшее значение метки безопасности Mi, i = 1, …, k им присваивается, т.е.: M1 < M2 < M3<…<Mk.

Таким образом, в качестве учетной информации субъектов и объектов доступа, кроме их идентификаторов – имен, каждому субъекту и объекту задаются метки безопасности из множества M. Контроль доступа диспетчером реализуется на основе правил, определяющих отношение линейного порядка на множестве M, где для любой пары элементов из множества M, задается один из типов отношения {>,<,=} (на практике реализуется выбор подмножества M, изоморфного конечному подмножеству натуральных чисел – такой выбор делает естественным арифметическое сравнение меток безопасности).

Рассмотрим правила анализа меток диспетчером доступа для модели полномочного контроля доступа. Для этого введем следующие обозначения:

- Ms – метка безопасности субъекта (группы субъектов) доступа;
- Mo – метка безопасности объекта (группы объектов) доступа;
- Метка безопасности с порядковым номером i – Mi устанавливается для субъекта доступа с порядковым номером i – Ci и для объекта доступа с порядковым номером i – Oi.

Правила (разрешения) состоят в следующем:

1. Субъект C имеет доступ к объекту O в режиме чтения в случае, если выполняется условие: Mc <, = Mo.

2. Субъект C имеет доступ к объекту O в режиме записи в случае, если выполняется условие: Mc = Mo.

Нетрудно увидеть, что в этом случае реализуется та же полномочная модель контроля доступа D (приведенная выше). На основании сказанного можем сделать следующий важный вывод.

Вывод. Мандатного принципа контроля доступа не существует как такового. Имеет смысл говорить о принципе полномочного контроля доступа. О механизме мандатного контроля доступа может идти речь лишь как о частном случае (частном решении) реализации полномочного контроля доступа, основанном на формализации назначения и анализа прав диспетчером доступа не на основе матрицы доступа, а на основе меток безопасности (или мандатов).

ПРИМЕНЕНИЕ ПОЛНОМОЧНОГО КОНТРОЛЯ ДОСТУПА ПРИ РЕШЕНИИ ЗАДАЧИ ПРОТИВОДЕЙСТВИЯ ВНУТРЕННИМ ИТ-УГРОЗАМ

Заметим, что именно для этой области приложений, в первую очередь, и был предложен данный принцип контроля доступа к ресурсам и именно он является основой реализации разграничительной политики доступа к ресурсам для данных приложений. Его применение состоит в следующем. Обработка информации различных категорий должна осуществляться на компьютере в различных режимах, причем, чем выше категория информации, тем жестче условия ее обработки, например, только открытая информация должна выдаваться во внешнюю сеть и т.д. Локализация режимов обработки информации различных категорий направлена на противодействие внутренним ИТ-угрозам, в части предотвращения возможности хищения категорированной информации санкционированным пользователем (инсайдером). Полномочный же контроль доступа к ресурсам в этих приложения служит для противодействия возможности понижения категории информации с той целью, чтобы она не могла быть обработана в несанкционированном для нее режиме, открывающем каналы ее хищения (мобильные накопители, электронная почта и т.д.), что иллюстрирует матрица доступа D, приведенная выше.

ЗАДАЧА ПРОТИВОДЕЙСТВИЯ ВНЕШНИМ ИТ-УГРОЗАМ

При построении и практическом использовании средства защиты необходимо учитывать, что задача защиты информации от НСД должна решаться в полном объеме, понимая, что эта задача состоит не только в защите от нарушения ее конфиденциальности (от несанкционированного раскрытия информации), но и в обеспечении ее доступности и целостности. А в этой части особое внимание следует обратить на противодействие внешним ИТ-угрозам, в частности, на противодействие возможному ее «заражению» (как следствие, нарушению целостности или вообще доступности информации) макровирусами.

Проиллюстрируем, в чем состоит особенность рассматриваемых приложений.

1. Обработка категорированной информации (например, «конфиденциально» и «открыто») априори предполагает, что, в первую очередь, объектом защиты является информация более высоких категорий (в частности, в первую очередь, следует защищать конфиденциальную информацию, работа с открытой информацией в данных приложениях является опциональной, и ее защита не столь важна).

2. Обработка категорированной информации (например, «конфиденциально» и «открыто») априори предполагает различные режимы создания, обработки и хранения информации различных категорий, причем чем выше категория информации, тем более жесткие ограничения накладываются на ее обработку (в частности, конфиденциальную информацию, как правило, разрешается создавать только на вычислительных средствах предприятия, причем определенным набором приложений, хранение и обмен данной информацией по сети, либо с использованием мобильных накопителей, также осуществляется между вычислительными средствами корпоративной сети, которые должны быть защищены, что требует обработка конфиденциальных данных, открытая же информация может поступать из непроверенных источников, не предполагающих реализации каких-либо регламентов по ее созданию, обработке и хранению). Как следствие, вероятность того, что «заражен» макровирусом открытый документ на порядки выше, чем конфиденциальный, соответственно, чем выше категория документа (жестче регламенты на режимы его обработки), тем меньше вероятность того, что документ «заражен» макровирусом.

Из всего сказанного можем сделать очень важный вывод: чем меньше категория документа, тем менее он нуждается в защите от «заражения», что в том числе сказывается на реализуемых режимах его обработки, как следствие, тем большей вероятностью быть «зараженным» он характеризуется.

С учетом же того, что на одном и том же компьютере обрабатывается как открытая (которая имеет большую вероятность «заражения»), так и конфиденциальная (которую необходимо защищать от «заражения») информация, может быть сформулирована задача антивирусной защиты в следующей постановке – обеспечить защиту конфиденциальных данных от макровирусов, которыми с большой вероятностью могут быть «заражены» открытые документы, т.е. предотвратить распространение вируса на конфиденциальные данные. В общем же случае (при наличии нескольких категорий конфиденциальности) задача может быть сформулирована следующим образом: предотвратить распространение вируса на данные более высокой категории конфиденциальности.

Для решения этой задачи нами предлагается кардинально иная реализация контроля доступа к ресурсам (вероятностный контроль доступа), где правила доступа субъектов к объектам формируются, исходя из значений (либо качественной оценки) вероятности «заражения» документов различных категорий макровирусами, целью которого является предотвращение возможности «заражения» документов более высокой категории макровирусами, априори хранящимися с определенной вероятностью в документах более низкой категории.

ВЕРОЯТНОСТНЫЙ КОНТРОЛЬ ДОСТУПА К РЕСУРСАМ

Как и ранее, будем считать, что чем выше полномочия субъекта и категория объекта, тем, соответственно, меньше их порядковый номер в линейно полномочно упорядоченных множествах субъектов и объектов – $C = \{C1,\ldots, Ck\}$ и $O = \{O1,\ldots, Ok\}$). Обозначим же через Pi вероятность того, что документ I категории «заражен» макровирусом, при этом (как было сказано выше) априори имеем: $P1 < P2 <\ldots< Pk$. Беря во внимание тот факт, что макровирус начинает действовать (что может нести в себе угрозу «заражения») лишь после прочтения его соответствующим приложением, и что предотвращать следует возможность «заражения» документа более высокой категории макровирусом из документа более низкой категории (после его прочтения приложением), получаем следующую матрицу доступа F, описывающую вероятностную модель контроля доступа, реализуемую для антивирусного противодействия:

	C1	C2	Ck-1	Ck
O1(P1)	Зп/Чт	Чт	Чт	Чт
O2(P2)	Зп	Зп/Чт	Чт	Чт
F = .	.....	.....	.....	.....
.	.....	.....	.....	.....
Ok-1(Pk-1)	Зп	Зп	Зп/Чт	Чт
Ok(Pk)	Зп	Зп	Зп	Зп/Чт

Видим, что при реализации данной модели контроля доступа разрешается запись документов, имеющих меньшую вероятность заражения макровирусом в объекты, документы в которых имеют большую вероятность «заражения» макро-вирусом – обратное запрещено, т.е. предотвращается повышение вероятности «заражения» документов более высокой категории конфиденциальности, за счет того, что одновременно с ними на одном и том же компьютере могут создаваться, обрабатываться и храниться документы более низкой категории, вероятность «заражения» макровирусом которых выше.

При реализации данной схемы вероятность «заражения» документа более высокой категории, например, O1 (P1) не изменяется в связи с тем, что на том же компьютере обрабатывается информация более низкой категории, например, Ok (Pk). При этом будем понимать, что режимы обработки информации различных категорий могут кардинально различаться (например, при обработке на одном компьютере открытой Ok и конфиденциальной информации O1, имеем: Pk >> P1, причем в зависимости от реализованных правил и организационных мер по обработке конфиденциальных данных это отношение может составлять сотни, тысячи и более раз, т.е. именно во столько раз можно снизить вероятность «заражения» конфиденциальных данных макровирусами, хранящимися в открытых данных, для которых порою Pk = 1).

Вывод. Вероятностный контроль доступа к ресурсам является эффективным средством противодействия внешним ИТ-угрозам, в частности, призван обеспечивать противодействие «заражению» конфиденциальных данных макровирусами. Высокая эффективность данная подхода обусловливается тем, что при его реализации противодействие макровирусам осуществляется в общем виде – не требуется выявления известных вирусов по их сигнатурам (т.е. противодействие оказывается как известным, так и неизвестным вирусам).

Сравним матрицы D и F. Видим, что они полностью противоречат друг другу, т.е. требования к реализации полномочного контроля доступа при решении альтернативных задач защиты информации (противодействие внешним и внутренним ИТ-угрозам) не то чтобы были различны – они противоречивы.

На основании сказанного можем сделать следующие важные выводы.

Вывод 1.

Полномочный контроль доступа (в частности, мандатный механизм контроля доступа) не позволяет решать задачу защиты информации от НСД в корпоративных приложениях. Применение данного способа, призванного обеспечивать противодействие внутренним ИТ-угрозам, т.е. противодействовать несанкционированному нарушению конфиденциальности информации, кардинально повышает вероятность внешней ИТ-угрозы, делая ее при обработке наряду с конфиденциальной открытой информации практически равной 1.

Вывод 2.

Вероятностный контроль доступа не позволяет решать задачу защиты информации от НСД в корпоративных приложениях. Применение данного способа, призванного обеспечивать противодействие внешним ИТ-угрозам, т.е. противодействовать несанкционированному нарушению доступности и целостности информации, кардинально повышает вероятность внутренней ИТ-угрозы, делая ее при обработке наряду с открытой конфиденциальной информации практически равной 1.

Вывод 3.

Рассмотренные специализированные подходы к решению задачи защиты компьютерной информации (полномочный и вероятностный принципы контроля доступа к ресурсам), не позволяют решать задачу защиты информации от НСД в корпоративных приложениях (позволяют решать лишь соответствующие частные задачи защиты, причем оказываемое ими противодействие одному типу ИТ-угроз, приводит к кардинальному повышению вероятности другого типа ИТ-угроз, т.е. одна задача защиты решается за счет другой).

КОМПЛЕКСНЫЙ ПОДХОД К РЕАЛИЗАЦИИ КОНТРОЛЯ ДОСТУПА К РЕСУРСАМ В КОРПОРАТИВНЫХ ПРИЛОЖЕНИЯХ.

Чтобы ответить на вопрос, как же быть – как совместить несовместимое (одновременно обеспечить противодействие раскрытию конфиденциальности информации и нарушению ее доступности и целостности, при одновременной обработке на одном компьютере открытой и конфиденциальной информации), т.е. **как решить задачу в комплексе,** прежде всего рассмотрим, какую информацию мы категорируем, применительно к решению задачи антивирусной защиты. Естественно, что качественное отличие в обработке имеет открытая информация и конфиденциальная информация, т.е. можем выделить две основные категории: «открыто» и «конфиденциально». При этом обработка конфиденциальной информации различных категорий, в части вероятности быть исходно «зараженной» макровирусом, уже отличается не столь существенно. С учетом сказанного на практике прежде всего имеет смысл рассматривать следующее отношение вероятностей того, что документ I категории «заражен» макровирусом, обозначив категорию «открыто» как k, имеем: P1 = P2 =…=Pk-1<<Pk.

Естественно, что если мы не можем разрешить ни чтения, ни запись (т.к. эти требования противоречивы в матрицах доступа), то остается лишь одно решение, связанное с полным запретом доступа. С учетом сказанного получаем модель полномочного контроля доступа, реализация которой позволяет решать рассмотренные альтернативные задачи в комплексе, описываемую матрицей доступа D(F):

$$D(F) = \begin{array}{c} \\ O1 \\ O2 \\ . \\ . \\ Ok-1 \\ Ok \end{array} \begin{array}{c} \begin{array}{cccc} C1 & C2.... & Ck-1 & Ck \end{array} \\ \begin{bmatrix} Зп/Чт & 0 & 0 & 0 \\ Чт & Зп/Чт & 0 & 0 \\ ..... & ..... & ..... & ..... \\ ..... & ..... & ..... & ..... \\ Чт & Чт & Зп/Чт & 0 \\ 0 & 0 & 0 & Зп/Чт \end{bmatrix} \end{array}$$

Заметим, что, по сути, при таком подходе к реализации полномочного контроля доступа обработка открытых данных полностью изолируется от обработки конфиденциальных данных. Результатом такого решения, никак не противоречащего идее обработки данных на основе полномочий пользователей и категорий объектов, является то, что повышение вероятности «заражения» макровирусом открытых данных никак не сказывается на вероятности «заражения» макровирусом конфиденциальных данных, что определяется условием: P1 =P2 =…=Pk-1<<Pk. Важным здесь является тот момент, что если на вероятность «заражения» макро-вирусом открытых данных повлиять практически невозможно, кроме как уменьшить ее значение, за счет применения специализированных антивирусных средств защиты (что, с одной стороны, не даст решения в общем виде, т.к. сигнатурный анализ позволяет находить только известные макровирусы, с другой стороны, в данных приложениях выглядит несколько странным – защищаем открытые данные, вообще говоря, не очень и нуждающиеся в защите, чтобы, в конечном счете, уберечь от «заражения» конфиденциальные данные), то вероятность «заражения» макровирусом конфиденциальных данных можно существенно снизить (на порядки – в сотни, в тысячи, а может быть, и более раз, реализовав соответствующие организационные мероприятия по ее обработке (которые и так априори должны быть реализованы, но уже с целью противодействия понижению категории информации).

Отметим, что матрица D(F) иллюстрирует тот факт, что при обработке на компьютере информации только двух категорий («открыто» и «конфиденциально» – наиболее распространенный случай), использование полномочного контроля доступа недопустимо.

В порядке замечания отметим, что в общем случае, используя рассмотренный подход (запрещая соответствующие права доступа), можно формировать различные правила контроля доступа (различные варианты защиты от «заражения» макровирусом конфиденциальных данных). Один из примеров соответствующей матрицы (изолируется обработка данных, наивысшей категории) доступа представлен ниже:

$$D(F) = \begin{array}{c} \\ O1 \\ O2 \\ . \\ . \\ Ok-1 \\ Ok \end{array} \begin{array}{c} \begin{array}{cccc} C1 & C2 ..... & Ck-1 & Ck \end{array} \\ \begin{bmatrix} Зп/Чт & 0 & 0 & 0 \\ 0 & Зп/Чт & 0 & 0 \\ ..... & ..... & ..... & ..... \\ ..... & ..... & ..... & ..... \\ 0 & Чт & Зп/Чт & 0 \\ 0 & Чт & Чт & Зп/Чт \end{bmatrix} \end{array}$$

$$D(F) = \begin{array}{c} \\ O1 \\ O2 \\ . \\ . \\ Ok-1 \\ Ok \end{array} \begin{array}{c} \begin{array}{cccc} C1 & C2 ..... & Ck-1 & Ck \end{array} \\ \begin{bmatrix} Зп/Чт & 0 & 0 & 0 \\ 0 & Зп/Чт & 0 & 0 \\ ..... & ..... & ..... & ..... \\ ..... & ..... & ..... & ..... \\ 0 & Чт & Зп/Чт & 0 \\ 0 & Чт & Чт & Зп/Чт \end{bmatrix} \end{array}$$

В порядке замечания отметим, что при условии: P1 << P2 <<…<< Pk-1 << Pk должна быть реализована каноническая модель контроля доступа.

С учетом сказанного можем сделать следующий важный вывод.

Вывод. При реализации комплексного подхода к решению задачи защиты информации (противодействие как внутренним, так и внешним ИТ-угрозам) в средстве защиты не должно быть реализовано какой-либо жестко заданной формализации отношений субъектов (пользователей) и объектов доступа на основе меток безопасности – задание правил разграничения доступа субъектов (пользователей) к объектам должно осуществляться на основе матрицы доступа, что позволяет совместить принципы полномочного и вероятностного контроля доступа к ресурсам, как следствие, эффективно решает задачу защиты компьютерной информации. Реализация какого-либо формализованного отношения приведет к тому, что оказываемое средством защиты противодействие одному типу ИТ-угроз приведет к кардинальному повышению вероятности другого типа ИТ-угроз, т.е. одна задача защиты будет решаться за счет другой.

Общий вывод по работе

При построении средства защиты компьютерной информации должен быть реализован комплексный подход, состоящий в том, что любое решение должно рассматриваться в комплексе – в свете того, как оно обеспечивает противодействие (либо влияет) как внутренним, так и внешним ИТ-угрозам. Только в этом случае может быть построено эффективное средство защиты информации. Это обуславливается тем, что при построении специализированного средства (не ориентированного на решение задач защиты информации в комплексе) одна задача защиты может решаться за счет другой, при этом оказываемое средством защиты противодействие одному типу ИТ-угроз приведет к кардинальному повышению вероятности другого типа ИТ-угроз (результирующая эффективность защиты подобного технического средства будет низка).

В заключение отметим, что рассмотренные в работе решения реализованы и апробированы в составе Комплексной системы защиты информации (КСЗИ) «Панцирь-К» для ОС Windows 2000/XP/2003 (разработка ЗАО «НПП «Информационные технологии в бизнесе», сертификат ФСТЭК №1144 от 17.01.2006). Более подробно с этой и с другими разработками ЗАО «НПП «Информационные технологии в бизнесе» читатель может познакомиться на сайте компании: www.npp-itb.spb.ru.