УДК 681.3.06

А.В. ПОТИЙ

ЗАО «Институт информационных технологий», Украина

ФОРМАЛЬНАЯ МОДЕЛЬ ПРОЦЕССА ЗАЩИТЫ ИНФОРМАЦИИ

В работе разрабатывается и предлагается для обсуждения вербальная и обобщенная формальная модель процесса защиты информации. Предлагаемые модели являются важными элементами процессного подхода к управлению защитой информации и формируют основу научно-методического аппарата управления защитой информации в рамках системодеятельносной методологии.

процессный подход, управление защитой информации, процесс защиты информации

Введение

Управление является основой обеспечения безопасности информации на объектах информационной деятельности. По определению управление представляет собой совокупность управляющих воздействий, выбранных субъектом управления из множества возможных воздействий на основе определенной информации и направленных на поддержание или улучшение функционирования объекта управления в соответствии с имеющейся стратегией и целью управления. Создание системы управления защитой информации основывается на последовательном определении объектов управления, целей и задач управления, показателей и критериев эффективности управления, функций управления, состава системы и организационной структуры управления, на разработке методов и средств управления. В рамках процессного подхода к управлению защитой информации [1] важно четко определить субъекты и объекты управления. Объектом управления является процесс защиты информации (ПЗИ) и его свойства, например зрелость, эффективность, экономическая эффективность и т.д. Субъектами управления являются активные участники процесса, взаимодействующие при выработке и принятии управленческих решений в ходе реализации и выполнения процесса. При решении задач управления важно иметь описание, модель объектов управления, которая отображает качественные характеристики объекта.

В данной работе предлагается вербальная и формальная модель процесса защиты информации. До настоящего времени в области защиты информации понятие процесс практически не использовалось, а если и использовалось, то без достаточного четкого определения. При разработке моделей автор исходит из признания того факта, что процессы защиты информации являются вспомогательными процессами, которые осуществляет организация для обеспечения эффективности своей основной деятельности, которая в современных условиях информатизации неизбежно предполагает использование критической информации. Опираясь на результаты, полученные в области моделирования бизнес-процессов в статье предлагается вербальная модель процесса, а затем и обобщенная формальная системная модель процесса.

1. Вербальная модель процесса защиты информации

Сущность процессного подхода заключается в том, что защита информации рассматривается как особый вид деятельности, осуществляемый в организации, который при моделировании, проектировании рассматривается как совокупность процессов защиты информации [2]. Единого определения понятия процесс в литературе не существует, . Однако анализ множества определений [3,4] позволяет выделить такие общие признаки процесса:

– наличие цели процесса, т.е. желаемого результата защиты информации, достигаемого при осуществлении процесса;

– изменения предметной области, в которой реализуется процесс. По сути, реализация процесса всегда связана с изменения некоторой системы, а является целенаправленным переводом этой системы из существующего в желаемое состояние;

– ограниченность требуемых ресурсов на выполнение операций и действий, входящих в состав процесса;

– непрерывность процесса. Процесс есть модель функции защиты, которая осуществляется организацией на протяжении всего своего существования;

– комплексность и разграничение процесса. Комплексность процесса предполагает учет всех внутренних и внешних факторов, прямо или косвенно влияющих на развитие процесса и результаты процесса. В то же время каждый процесс имеет четко определенные рамки своей предметной области, например процесс анализа угроз, процесс сертификации средств защиты, процессы стратегического управления безопасностью и т.д.

При формировании определения понятия ПЗИ необходимо учесть особенности предметной области защиты информации, результаты анализа отношений между понятиями «защита информации», «меры защиты информации» и «процесс защиты информации», которые рассматривались с позиций системодеятельносного подхода к защите информации [5].

Анализ определений процесса и признаков процесса позволил нам предложить следующее определение.

Определение 1. ПЗИ это совокупность взаимосвязанных операций и действий, направленных на реализацию взаимоувязанного комплекса мер защиты информации на основе определенной технологии (техники) защиты путем преобразования входных материальных и информационных потоков в выходные потоки, представляющие интерес для субъекта защиты информации.

ПЗИ реализуется и протекает в соответствии с управляющими директивами (воздействиями) и правилами (политикой) безопасности, которые вырабатываются на основе общих и частных целей и задач защиты информации. В определении ПЗИ учитывается потребность субъекта защиты информации в реализации мер защиты информации. При моделировании процессов защиты информации, меры защиты информации могут рассматриваться как функции защиты на организационном уровне.

Представленное выше определение ПЗИ позволяет рассматривать защиту информации как совокупность процессов. Защита информации осуществляется в соответствии с заранее определенной и постоянно корректируемой целью защиты и связана с затратами финансовых, энергетических, трудовых, материальных и иных ресурсов, при учете ограничений со стороны внешней среды. Желаемый результат защиты информации достигается более эффективно, когда связанные ресурсы и деятельность рассматриваются и управляются как процесс.

Процесс, как категория, используется нами в качестве средства структурирования деятельности субъекта защиты информации. Структуризация деятельности осуществляется исследователем ради достижения определенных целей и решения определенных задач, например, в целях моделирования, анализа, проектирования и т.д. Такое структурирование деятельности осуществляется посредством таких понятий как меры защиты информации, ПЗИ, операция и действия по защите информации. Все эти понятия могут быть объединены таким общим понятием как практика защиты информации.

Практическая полезность этих понятий устанавливается в ходе решения конкретных задач защиты. Наша позиция заключается в том, что в процессном подходе при анализе слабоструктурированной деятельности по защите информации основополагающую роль играет понятие процесса. Представление деятельности через совокупность процессов – основной способ системного представления деятельности на современном этапе развития методологи-

ческих подходов к решению проблем защиты информации.

Деятельность по защите информации, реализация и выполнение определенных процессов защиты информации происходит в окружении некоторой динамической среды, которая оказывает на него определенное воздействие. При проектировании (моделировании) и выполнении процесса необходимо определить и учесть все возможные на него воздействия: экономические, социальные, финансовые, организационные и пр.

Определение 2. Окружение процесса – среда процесса, порождающая совокупность внутренних и внешних сил, которые способствуют или мешают достижению целей процесса.

Факторы окружения процесса необходимо проанализировать и выделить из них те, которые могут оказать на выполнение процесса заметное влияние. Процесс нельзя отделять от этих окружающих условий и их развития. Необходимо заблаговременно учитывать непосредственное окружение процесса (предприятие, организацию, учреждение, в котором выполняется процесс) и дальнее окружение процесса (окружение предприятия, организации, учреждения).

Процессы реализуются для достижения определенных целей защиты и получения конкретных результатов в интересах определенных субъектов, участвующих в проектировании, реализации и выполнении процесса защиты информации.

Определение 3. Участники процесса защиты информации это физические лица и организации, которые непосредственно вовлечены в реализацию процесса или чьи интересы могут быть затронуты в ходе выполнения процесса.

Состав участников процесса, их роли, функции, полномочия, обязанности и ответственность зависят от различных факторов, таких как тип, вид процесса, фазы жизненного цикла процесса и пр.

В результатах процесса защиты информации заинтересован субъект защиты информации. С точки зрения процесса он выступает в роли *владельца процесса*. *Владелец процесса* это субъект, который осознал свои потребности в обеспечении безопасности информации и необходимость решения задач защиты, т.е. имеет потребности в конкретных результатах, обладает мотивом к реализации и выполнению процесса и располагает ресурсами и необходимыми процедурами, технологиями и механизмами для реализации и выполнения процесса. В роли субъекта-владельца процесса может выступать как физическое лицо, так и организация, общество, государство.

Процесс должен разрабатываться и выполняться, значит среди участников процесса выделяются *субъекты-исполнители* процесса.

В результате выполнения процесса формируются результаты, у которых есть свои потребители. Для выполнения процесса на его вход должны поступить определенные материальные или информационные объекты, у которых есть свои поставщики. Поэтому среди участников процесса можно выделить *субъекты-потребители* и *субъекты-поставщики*.

Важными понятиями является вход и выход процесса.

Определение 4. Выход процесса есть поток материальных или информационных объектов (продуктов), являющийся результатом выполнения процесса и потребляемый внешними по отношению к процессу объектами.

Выход процесса защиты информации всегда имеет потребителя, именно поэтому результат процесса мы можем рассматривать как продукт. Потребителем может выступать в частности другой процесс, для которого выход первого является входом. Выход процесса может использоваться в качестве ресурса для выполнения другого процесса. К выходам процессов защиты информации могут относиться документация, информация, требования безопасности, новое состояние объекта информатизации и т.д.

Определение 4. Вход процесса – это поток материальных или информационных объектов (продук-

тов), который в ходе выполнения процесса преобразуется в выход.

Определение 5. Ресурс процесса – материальный или информационный объект, постоянно используемый для выполнения процесса, но не являющийся входом процесса.

К ресурсам процесса защиты информации могут относиться: информация, персонал, оборудование, техника защиты, программное обеспечение, инфраструктура, среда, телекоммуникации и т.д.

Если рассматривать процесс как объект управления, то среди участников процесса необходимо выделить должностное лицо, ответственное за выполнение процесса и его результат. Такое должностное лицо называется *управляющим процесса*. Чтобы управляющий процессом мог управлять процессом, в его распоряжение необходимо выделить ресурсы, необходимые для осуществления процесса, делегировать права и полномочия. Управляющий процессом в ходе планирования, управления и усовершенствования процесса осуществляет распределение и перераспределение ресурсов для достижения наилучшей эффективности процесса, основными составляющими которой является результативность и экономичность, а также достижения требуемой зрелости процесса. Каждый процесс существует не сам по себе, а выполняет какие-либо функции защиты в рамках системы процессов и является подконтрольным высшему руководству организации. Управляющий процессом несет ответственность за результаты процесса перед владельцем процесса. В общем случае процессом может управлять не одно лицо, а коллегиальный орган управления. Исходя из этого, введем следующее определение управляющего процессом, как субъекта управления.

Определение 6. Управляющий процессом – это должностное лицо или коллегиальный орган управления, имеющий в своем распоряжении ресурсы, необходимые для выполнения процесса и несущий ответственность за результаты процесса перед владельцем процесса.

2. Формальная модель процесса защиты информации

В [6] предлагается формально определить процесс как последовательность действий в некотором пространстве состояний и описывать тройкой вида:

$$P = (\mathrm{Z}, f, s) \qquad (1)$$

где Z – пространство состояний; f – функция действия (переходов); s – множество начальных состояний.

Данная модель являются весьма обобщенной, и не отражает многие аспекты, указанные нами при формировании вербальной модели. В модели (1) учитывается состояние системы, но не учитывает входные и выходные воздействия. Кроме того, при рассмотрении управления данная модель неизбежно должна быть подвергнута модификации. По сути приведенная модель больше описывает модель окружения процесса. Общая схема воздействия внешних и внутренних факторов на выполнение процесса представлена на рис. 1.

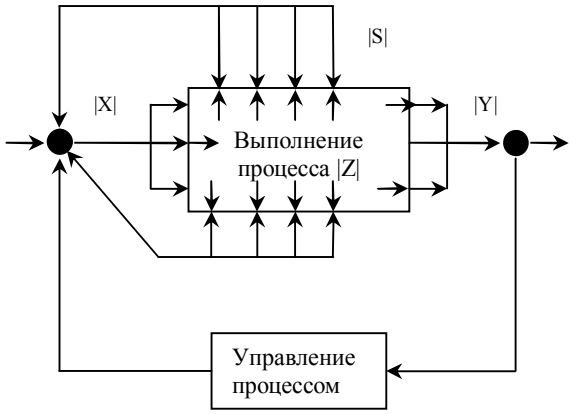

Рис. 1. Общая схема воздействия внешних и внутренних факторов на процесс: $|X|$ – вектор начальных условий; $|Y|$ – вектор конечных условий; $|S|$ – вектор воздействий внешнего окружения; $|Z|$ – вектор факторов внутренней среды процесса

В основу предлагаемой формальной модели процесса положим следующие аксиоматические конструкции.

А1. Набор (множество) операций и действий $\mathbf{O} = \{o_1, o_2, \ldots o_n\}$ по защите информации, составляющие ПЗИ P.

А2. Множество отношений $\mathbf{R} = \{r_1, r_2, \ldots r_m\}$ различного типа, определенных на множестве $\mathbf{O}$.

Множество операций $\mathbf{O}$ образует процесс $P(\mathbf{O}, r)$, если $\mathbf{O} \in \overline{\mathbf{O}}$ и на этом множестве задано отношение $r(\mathbf{O}) \in \mathbf{R}$. Здесь $\overline{\mathbf{O}}$ - универсальное множество действий по защите информации. Для каждого процесса $P(\mathbf{O}, r)$ отношение $r(\mathbf{O})$ будем называть структурой процесса. Для образования процесса необходимо как минимум на множестве $\mathbf{O}$ задать отношение порядка. Тогда множество операций может интерпретироваться как последовательность операций.

А3. Цель Tar и ожидаемые результаты процесса Rez формируют назначение процесса

$$Pur = \langle Tar, Rez \rangle . \qquad (2)$$

Процесс реализуется и выполняется для достижения цели и получения конкретного результата, представляющие интерес для участников процесса. Цель является фактором, который определяет отношения на множестве операций и выступает системообразующим фактором. Цель может быть задана и множеством целей с заданным на этом множестве отношением иерархии.

А4. Множество входов $IN = \left\{ I^{in}, M^{in} \right\}$ и выходов $OUT = \left\{ I^{out}, M^{out} \right\}$ процесса P с заданным оператором преобразования $F : IN \to OUT$.

В общем случае входы и выходы процесса могут представлять собой материальные и информационные объекты. Материальный поток M представляет собой непрерывное или дискретное множество материальных объектов $M = \left\{ m_1, m_2, \ldots, m_q \right\}$, распределенных во времени.

Информационный поток I представляет собой непрерывное или дискретное множество информационных объектов $I = \left\{ i_1, i_2, \ldots, i_q \right\}$.

В соответствии с методологией IDEF0 выделяют ограничительную информацию $I^{огр}$, описательную информацию I^{on} и управляющую информацию $I^{упр}$.

Ограничительная информация $I^{огр}$ представляет собой сведения запрещающего характера, которые содержаться в законах, подзаконных актах, международных, государственных и отраслевых стандартах, а также в специальных внутренних положениях и документах организации (политика безопасности, инструкции, требования, регламенты и т.д.), в рамках которой выполняется процесс.

Описательная информация I^{on} представляет собой сведения об атрибутах объектов, которые подаются на вход и формируются на выходе процесса P и преобразуется в результате выполнения процесса. Описательная информация может содержаться в чертежах, технических и иных описаниях, реквизитах и других документах и является неотъемлемым компонентом объекта в течение всего жизненного цикла.

Управляющая (предписывающая) информация $I^{упр}$ представляет собой сведения о том, как, при каких условиях и по каким правилам следует осуществлять преобразование входного объекта (потока) IN в выходной объект (поток) OUT. Управляющая информация содержится в технологических инструкциях, руководствах, документах, командах и т.п., которые определяют «настройки» и характеристики оператора преобразования F и процесса P в целом.

А5. Множество участников-субъектов процесса

$$PS = (Own, Man, Per, Sup, Cus,), \qquad (3)$$

где Own - владелец процесса; Man - управляющий процессом; Per - исполнитель процесса; Sup - поставщик процесса; Cus - потребитель процесса.

Множество участников процесса образуют команду процесса $Process\_Team$, если на множестве PS определены роли $role$ и полномочия $authority$ субъектов процесса, которые характеризуют отношения между участниками процесса, т.е.

$$\text{Process}\_Team(PS, role, authority) \qquad (4)$$

А6. Множество финансовых, временных, трудовых, экономических, материальных и иных ресурсов, необходимых для реализации и выполнения процесса P:

$$\text{Resource} = \{\text{F, T, L, E, Mat}\}. \quad (5)$$

Введенные аксиоматические конструкции позволяют предложить формальную модель процесса

$$P = \left\langle \begin{matrix} Pur, r(\mathbf{O}), F : IN \to OUT, \\ \text{Process}\_Team, \text{Resource} \end{matrix} \right\rangle. \quad (6)$$

Данная модель может рассматриваться как базовая для дальнейших исследований.

Заключение

Сегодня вопросы управления являются одними из актуальных вопросов в области защиты информации, что демонстрируется вниманием к этим вопросам в международных стандартах. Однако вопросам разработки научных и методических основ управлению защитой информации, к сожалению, уделяется недостаточное внимание.

Один из основополагающих принципов обеспечения безопасности информации требует, чтобы управление защитой информации было интегрированной частью общего управления организацией. В работе развивается процессный подход к управлению защитой информации, как наиболее приемлемый способ реализации указанного принципа. На основе анализа множества определений бизнес-процессов, анализа сущности защиты информации как особого вида деятельности, в работе разрабатывается вербальная модель процесса защиты информации, формируется понятийный аппарат управления процессами защиты информации. Это является важным этапом на пути формирования методических и теоретических основ управления защитой информации.

Для изучения свойств процесса, разработки различных моделей процесса (например, моделей зрелости, эффективности и т.п.), разработки системы процессов защиты информации в работе предлагается обобщенная системная модель процесса, которая определяет основные качественные характеристики процесса и формализует его основные элементы. Дальнейшее уточнение модели позволит исследователям концентрировать внимание на том или ином аспекте изучение такой категории как ПЗИ.

Литература

1. Потій О.В. Процесний підхід до управління безпекою інформації // VIII Международная научно-практическая конференция "Безопасность информации в ІТС", 11-13 мая 2005. Тезисы докладов. – К.:НИЦ "Тезис", 2005. – С. 35-36.

2. Потий А.В. Управление безопасностью информации: сущность и базовые принципы // VIII Международная научно-практическая конференция "Безопасность информации в ИТС", 11-13 мая 2005. Тезисы докладов. – К.:НИЦ "Тезис", 2005. – С. 69-70.

3. Арчибальд Р. Управление высокотехнологичными программами и проектами. – М.: Компания АйТи; ДМК Пресс, 2004. – 472 с.

4. Шафер Д.Ф., Фатрелл Р.Т., Шафер Л.И. Управление программными проектами: достижения оптимального качества при минимуме затрат. – М.: ИД «Вильямс», 2003. – 1136 с.

5. Бондаренко М.Ф., Потий О.В. Визначення та обґрунтування суті політики інформаційної безпеки // Радиотехника. Всеукраинский межвед. научн.-техн. сб. – Х.: ХНУРЭ, 2003. – Вып. 134. – С. 9-25.

6. Schwickert C, Fisher K. Der Geschaftsprozeb als formaler Prozeb – definition, eigenschafte und arten. Arbeitspiere 4, BWL, 1996.

Поступила в редакцию 14.02.2006

Рецензент: канд. техн. наук, проф. А.А. Замула, Харьковский национальный университет радиоэлектроники, Харьков.