УДК :6813.06

ЭТАЛОННАЯ МОДЕЛЬ СИСТЕМЫ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

Александр Потий
ЗАО «Институт информационных технологий», Украина

Анотація: **Запропонована концепція процесного підходу до управління захистом інформації. Викладаються основні положення та сутність процесного підходу, запропонована вербальна та формальна моделі процесу захисту інформації. Обґрунтовані та пропонуються до застосування нові визначення та терміни в галузі захисту інформації. Обґрунтована еталонна модель процесів захисту інформації – дім процесів захисту інформації. Формуються основи науково-методичного апарату процесного управління захистом інформації.**
Summary: **In this article conception of process approach to information security management were proposed. Framework and essence of process approach were carried out, verbal and formal models of information security processes were proposed. New information security definitions and terms well-founded and proposed to use.**
Ключевые слова: **Процессный подход, меры защиты инормации, эталонная модель процессов защиты информации.**

Введение

В данной работе рассматриваются основные положения и концепция процессного подхода в области защиты информации (ЗИ). Процессный подход в целом охватывает терминологическую систему процессного подхода, базовую модель процесса ЗИ и управления процессом, эталонную системную модель процессов ЗИ, модели зрелости процессов ЗИ, методы оценки эффективности, результативности и зрелости процессов ЗИ. До настоящего времени в области ЗИ 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 ЗИ для организации являются вспомогательными процессами, которые осуществляется организацией для обеспечения эффективности своей основной деятельности. Опираясь на результаты, полученные в области моделирования бизнес-процессов, предлагается вербальная модель процесса, обобщенная формальная системная модель процесса и обосновывается эталонная модель системы процессов ЗИ в организации.

I Основные положения и концепция процессного подхода к управлению ЗИ

На сегодняшний день такие понятия, как «процессный подход», «процессное управление», «процессный подход в управлении» в области ЗИ четкого и строгого определения не имеют. Анализ многочисленных публикаций по процессному подходу в менеджменте, моделированию бизнес-процессов, внедрению систем сбалансированных показателей показал, что в современном менеджменте технология процессного подхода рассматривается как один из современных альтернативных механизмов системы создания эффективного управления организацией. В области управления ЗИ данные подходы еще не применяются.

Освоение и применение предлагаемой концепции на практике позволит:

1) сформировать комплексный взгляд на проблему обеспечения безопасности информации в целом и управления ЗИ в частности в различных организационных и организационно-технических системах;

2) разработать и реализовать способы решения проблем и задач управления ЗИ при помощи научно-методического аппарата процессного подхода;

3) внедрить процессный подход в практическую деятельность организации по ЗИ;

4) обеспечить условия постоянного улучшения деятельности по ЗИ.

Процессный подход к управлению ЗИ необходимо рассматривать как альтернативный механизм улучшения деятельности организации по ЗИ. Каковы же типичные ситуации, сложившиеся в области обеспечения безопасности информации на современных предприятиях, особенно ИТ-предприятиях, которые подталкивают руководителей предприятия к использованию процессного подхода как средства улучшения деятельности по ЗИ?

Первая ситуация характеризуется тем, что скорость роста применения современных информационных технологий в деятельности различных организаций, увеличение объема критической информации, увеличение парка систем и средств ЗИ опережает скорость развития системы управления ЗИ. Складываются условия, при которых риск потери управляемости системы защиты становится

неприемлемым. Руководители подразделений ЗИ начинают искать новые способы удержания ситуации под контролем путем описания и автоматизации деятельности (процессов) по ЗИ.

Вторая ситуация характеризуется тем, что происходит перестройка системы управления основной деятельностью организации на основе принципов процессного подхода. Это приводит к необходимости изменения и вспомогательных видов деятельности, к которым в частности относится деятельность по ЗИ.

Таким образом, побудительные мотивы руководителей подразделений по ЗИ, могут формироваться как под давлением внутренних факторов, связанных с естественным развитием системы ЗИ, так и под влиянием внешних факторов, связанных с общим развитием деятельности организации.

Опыт работы с крупными государственными компаниями и учреждениями, общение с руководителями подразделений по ЗИ, анализ состояния деятельности по ЗИ в различных организациях позволили автору сделать важный вывод: не все руководители высшего и среднего звена управления могут достаточно четко сформулировать свои пожелания и потребности в ЗИ, а тем более сформулировать четкие требования безопасности. Но у большинства из них сложилось ясное понимание необходимости искать способы решения управленческих проблем в области ЗИ.

От применения процессного подхода к управлению ЗИ можно ожидать решения таких проблем:

- снижение издержек на реализацию мер ЗИ;
- повышение уровня управляемости системы ЗИ (улучшение системы отчетности в области ЗИ, системы планирования и контроля ЗИ, создания прозрачной системы управления, ускорение процедур принятия решения и т. д.);
- повышение уровня защищенности и безопасности критических информационных активов и других, связанных с информацией, ресурсов организации;
- снижение уровня влияния субъективного (человеческого) фактора при реализации мер и управлении деятельностью по ЗИ.

В основу концепции процессного подхода к управлению ЗИ заложены.

1. Принципы обеспечения безопасности информации [7], принципы практической деятельности по ЗИ [8], принципы построения систем управления качеством [9].

2. Модель процесса ЗИ как основного элемента структурирования и описания деятельности по ЗИ.

3. Цикл Деминга-Шухарта PDCA [11], который используется как методологическая основа управления процессами ЗИ и стандартный жизненный цикл системы ЗИSDLC [7], используемый для связи процессов ЗИ с процессами проектирования и эксплуатации систем ЗИ.

4. Принципы и подходы построения систем показателей безопасности, в частности метрических показателей ЗИ и сбалансированной системы показателей деятельности по ЗИ на основе методологии BSC Нортона-Каплана [10].

5. Принципы и методология управления проектами, поскольку любые изменения в организации, в том числе и внедрение процессного подхода, усовершенствование процессов ЗИ должны реализоваться как высокотехнологичный проект [3, 4].

6. Модель зрелости процессов ЗИ.

Сущность процессного подхода заключается в том, что ЗИ рассматривается как особый вид деятельности, осуществляемый в организации, который при моделировании, проектировании рассматривается как совокупность процессов ЗИ [2]. В основе процессного подхода к управлению ЗИ лежит выделение в организации процессов ЗИ, которые представляют собой содержание особого вида деятельности организации – деятельности по ЗИ, и выделение управления этими процессами.

Дальнейшие исследования в данной области мы строим на следующих предположениях.

Предположение 1. Основные принципы обеспечения безопасности информации и принципы менеджмента не зависят от типа, профиля и области деятельности организации. Термин «организация» в равной степени применим для промышленного предприятия, государственного учреждения, органа управления, частной фирмы (компании), коммерческой или государственной структуры.

Предположение 2. Для всех типов организаций актуальной задачей является построение эффективной системы управления ЗИ, которая будет обеспечивать достижение целей безопасности информации, решение задач защиты и поддерживать достижение успеха организации в целом.

II Понятие и вербальная модель процесса ЗИ

Для формирования определения процесса ЗИ, рассмотрим определения понятия процесса как такового. На сегодняшний день единого определения понятия процесс или бизнес-процесс нет. Понятие «процесс», которое используется в самых различных сферах человеческой деятельности, является достаточно широким и нестрогим. Именно поэтому трудно дать определение, которое относилось бы ко всем видам процессов без исключения, и одновременно четко выделяло бы их среди объектов другой природы. Л.

Витгенштейн в теории определений относительно таких очень широких понятий говорил о наличии, скорее не общности всех разнообразных объектов, которые охватываются понятием, а об их «семейном сходстве». В табл. 1 представлены различные определения понятия процесс.

Таблица 1. Определения понятия «процесс»

Определение	Источник
1) Природное явление, которое отличается поступательными изменениями, приводящими к особенному результату; природная непрерывная деятельность или функция. 2) Совокупность действий или операций, которые приводят к результату	Словарь Вебстера
Процесс – закономерное, последовательное изменение явления, его переход в другое явление	Философский словарь
Процесс – это специальным образом упорядоченная во времени и пространстве совокупность рабочих действий, которая имеет начало и конец	Толковый словарь по информатике
Процесс – совокупность различных видов деятельности, в рамках которой "на входе" используются один или более видов ресурсов, и в результате этой деятельности на "выходе" создается продукт, представляющий ценность для потребителя	Hammer, Champy, 1993
Набор логически взаимосвязанных действий, выполняемых для достижения определенного выхода бизнес-деятельности	Davenport, Short, 1990
Структурированное конечное множество действий, спроектированных для производства специфической услуги (продукта) для конкретного потребителя или рынка. Или – специфически упорядоченная совокупность работ, заданий во времени и в пространстве с указанием начала и конца и с точным определением входов и выходов. Или – структурируемый, измеряемый набор действий, созданный, чтобы произвести определенный выход для конкретного клиента или рынка	Davenport, 1993
Сущность, определяемая через точки входа и выхода, интерфейсы и организационные устройства, частично включающие устройства потребителя услуг\товаров, в которой происходит наращивание стоимости производимой услуги\товара	Porter, Millar,1985
Множество внутренних шагов (видов) деятельности, начинающихся с одного и более входов и заканчивающихся созданием продукции, необходимой клиенту (просто клиент или процесс, протекающий во внешнем окружении компании) и удовлетворяющей его по стоимости, долговечности, сервису и качеству. Или – полный поток событий в системе, описывающий, как клиент начинает, ведет и завершает использование бизнеса	Ойхман, Попов, 1997
Логические серии взаимозависимых действий, которые используют ресурсы предприятия для создания или получения в обозримом или измеримо предсказуемом будущем полезного для заказчика выхода, такого как продукт или услуга	Зиндер, 1996
Горизонтальная иерархия внутренних и зависимых между собой функциональных действий, конечной целью которых является выпуск продукции или отдельных ее компонентов	Верников, 1999
Любые виды деятельности в работе организации	Deming, 1982
Действие, переводящее вход системного объекта в выход	Никаноров, 1969
Процесс – взаимосвязанный набор действий (операций, функций), которые по определенным правилам преобразуют исходные экономические ресурсы в конечные продукты или услуги	ВПТ02
Процесс – это устойчивая, целенаправленная совокупность взаимосвязанных видов деятельности, которая по определенной технологии преобразует входы в выходы	Елиферов- Репин
Систематизированное последовательное исполнение функциональных операций, которые приносят специфический результат	TeleManagement ab

Совокупность взаимосвязанных ресурсов и деятельности, которая преобразует входящие элементы в выходящие	Госстандарт, 1997
Ряд взаимосвязанных видов деятельности, преобразующих входы в выходы. Или – множество взаимосвязанных и взаимодействующих операций, которые преобразуют входы в выходы	ISO/IEC 9000: 2001.
Последовательность этапов, которые выполняются для достижения конкретной цели	ISO/IEC IEEE610
Последовательность взаимосвязанных видов деятельности, которые преобразуют входы на выходы	ISO/IEC 15504
Множество из одной или нескольких связанных операций или действий, которые в случае коллективного осуществления реализуют бизнес-задачи или политические цели, обычно в рамках организационной структуры, которая определяет функциональные роли и взаимоотношения между субъектами процесса	Стандарт WfMC
Процесс – это совокупность операций, выполняющихся последовательно или параллельно и преобразующих материальный и/или информационные потоки в соответствии с управляющими директивами, которые вырабатываются на основе целей деятельности. В ходе процесса потребляются финансовые, энергетические, трудовые и материальные ресурсы и выполняются ограничения со стороны других процессов и внешней среды	РД IDEF0

Исходя из концепции системодеятельного подхода к ЗИ, наиболее приемлемым для анализа понятия процесса ЗИ является определение его как совокупности действий или операций, которые приводят к некоторому результату. В роботе [12] определяются такие ключевые свойства «сущности, которую мы называем процессом:

- он содержит целенаправленные действия (т. е. выполняется для достижения цели);
- он осуществляется объединенной группой субъектов (т. е. процесс это нечто большее, чем индивидуальная работа);
- он пересекает функциональные границы организации;
- он постоянно управляется извне (процесс всегда имеет потребителя).

В работе [13] процесс определяется как «транзакция или последовательность транзакций между объектами, т. е обмен услугами или сообщениями». Здесь автор выявил коммуникационную функцию процесса. Отметим, что под коммуникацией мы понимаем связь между двумя или несколькими объектами, которая основана на передаче информации.

В 1994 году Snowdon и Warboys [14] предложили такое толкование процесса: «Организация в своей деятельности использует определенные «активы» (финансовые, интеллектуальные, материальные и т. д.) для наращивания ценности своих «выходов» и для того, чтобы производить эти «выходы», которые, в свою очередь, непосредственно или косвенно увеличивают активы организации и приносят доход. Это мы и называем процессом». В этом определении аспект делается на полезности для организации результатов, формирующихся процессом. Этому толкованию созвучны определения Hammer, Champy, Porter, Millar (см. табл. 1)

С конца 90-х годов активно развивается теория и практика управления проектами в различных сферах деятельности. Особенно активно методы управления проектами использовались в программной инженерии, связи и телекоммуникациях, аэрокосмической, автомобильной промышленности и в других высокотехнологичных сферах деятельности. С точки зрение управлениями проектами процесс – это ограниченный ряд взаимосвязанных действий, в ходе осуществления которых используется один или более входных продуктов (артефактов), а потом, с помощью одного или нескольких преобразований, создается выходной продукт (артефакт), который представляет ценность для заказчика. Таким образом, процесс представляет собой совокупность действий, инструментов, методов и технологий, в ходе осуществления и применения которых входные артефакты преобразуются в выходные артефакты. В качестве входов и выходов процесса может рассматриваться информация, материалы, энергия. При этом величина входа, в общем случае, должна быть меньшей, чем величина выхода. В таком же контексте понимают процессы международные и промышленные стандарты (см. табл. 1)

Обобщая все эти определения можно сказать, что процесс, как категория, используется для того, чтобы структурировать деятельность субъектов деятельности (человека, группы людей, организации и т. д.) в любой сфере. Разделение деятельности на составные части есть чисто условным, и осуществляется исследователем ради достижения определенной цели или решения определенных задач. Такое

структурирование деятельности осуществляется с помощью общих понятий, практическая ценность которых устанавливается в ходе решения задач. С другой стороны, процесс есть совокупность взаимосвязанных операций и действий, объединенных единством цели и функциональной целостностью, преобразующих входные потоки в выходные. Здесь явно просматриваются системные признаки процесса и, следовательно, деятельности, как совокупности процессов.

В процессном подходе к ЗИ как виду специфической деятельности организации определение общего понятия процесса ЗИ играет основополагающую роль. Понятие процесса ЗИ является одним из способов моделирования ЗИ наряду с другими ее представлениями.

Анализ приведенных и рассмотренных нами определений подтверждает вывод о том, что на сегодняшний день единого определения процесса не существует и вряд ли целесообразно вообще давать такое определение. В конкретных приложениях, сферах деятельности формируется свое определение, которое наполняется конкретным смыслом, наиболее полно соответствует представлению исследователя и применимо для описания и моделирования процессов. Однако анализ множества определений позволяет выделить такие общие признаки процесса, которые мы отразим с точки зрения содержания ЗИ:

- наличие цели процесса, т. е. желаемого результата ЗИ, достигаемого при осуществлении процесса;
- изменения предметной области, в которой реализуется процесс; по сути, реализация процесса всегда связана с изменения некоторой системы, и 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.

С одной стороны, при формировании определения понятия процесса ЗИ мы будем исходить из общих положений системодеятельного подхода к ЗИ, в котором категория «деятельность» является основополагающей. При раскрытии понятия процесса ЗИ необходимо учесть особенности предметной области ЗИ, результаты анализа отношений между понятиями «ЗИ», «меры ЗИ» и «процесс ЗИ», которые рассматривались с позиций системодеятельносного подхода к ЗИ [1, 2, 5]. На рис. 1 предлагается информационная (концептуальная) модель, характеризующая отношения между вышеназванными понятиями.

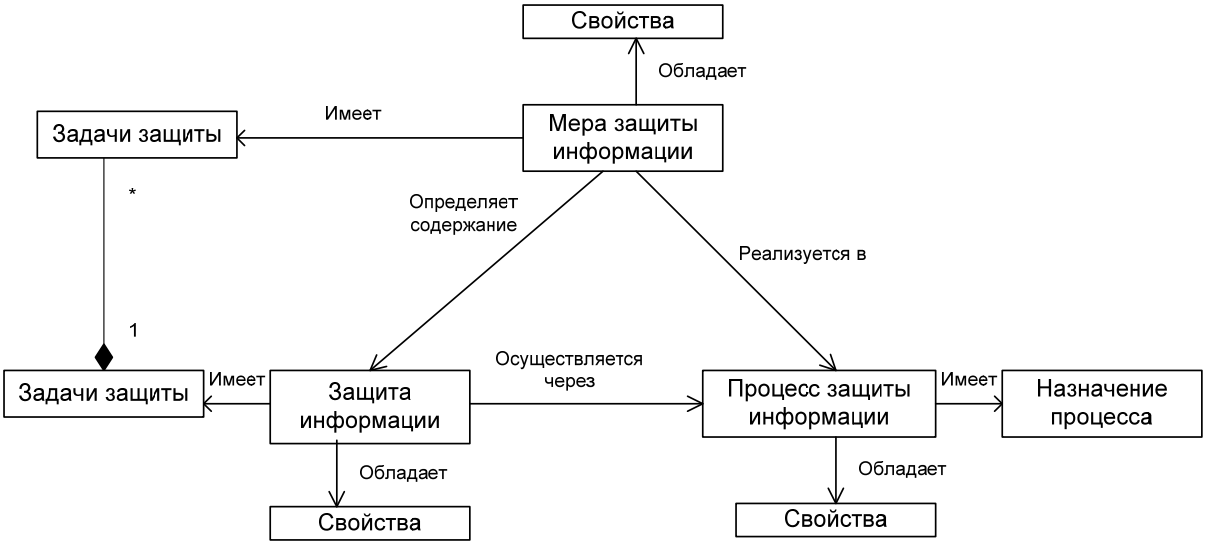


Рисунок 1 – Информационная модель типа «сущность-отношение» для категорий «защита информации», «меры защиты информации», «процесс защиты информации»

Введем определения ЗИ и меры ЗИ в рамках системодеятельного подхода.

Определение 1. ЗИ – это систематическая, стабильная и целенаправленная деятельность субъекта ЗИ (человека, организации, государства) относительно достижения целей ЗИ и решения основных задач ЗИ (обеспечения конфиденциальности, доступности, целостности и наблюдаемости информации и систем), а также обеспечения требуемого уровня доверия (гарантий).

Определение 2. Мера ЗИ – политики (правила), процедуры, действия, технологии и организационные структуры, предпринятые субъектом ЗИ в отношении объектов защиты (защищаемой информации, информационной системы, объекта информационной деятельности, организации, ведомства), с целью решения конкретных задач защиты.

Другим аспектом, который учитывается нами при формировании понятия процесса ЗИ является общая классификация функций организационных, организационно-технических и производственных систем с точки зрения их моделирования в рамках методологий SADT [15], IDEF0 [16] и ARIS [17 – 19]. Это позволяет уточнить место процесса среди таких понятий, как «деятельность», «операция», «действие».

Наконец, определение процесса ЗИ формулируется с учетом терминологических систем, которые представлены в стандартах ГОСТ Р 50922-96, НД ТЗИ 1.1. – 001 – 99 и других национальных и международных стандартах.

С учетом результатов анализа определений процесса, содержания понятия «процесса» вообще, признаков процесса в работе предлагается следующее определение процесса ЗИ.

Определение 3. Процесс ЗИ – это совокупность взаимосвязанных операций и действий, направленных на реализацию взаимоувязанного комплекса мер ЗИ на основе определенной технологии (техники) защиты путем преобразования входных материальных и информационных потоков в выходные потоки, представляющие интерес для субъекта ЗИ.

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

Представленное выше определение процесса ЗИ позволяет рассматривать ЗИ как совокупность процессов. ЗИ 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 ЗИ достигается более эффективно, когда связанные ресурсы и деятельность рассматриваются и управляются как процесс.

Процесс, как категория, используется нами в качестве средства структурирования деятельности субъекта ЗИ. 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 ЗИ, процесс ЗИ, операция и действия по ЗИ. Все эти понятия могут быть объединены таким общим понятием, как практика ЗИ.

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 ЗИ основополагающую роль играет понятие процесса. Представление деятельности через совокупность процессов – основной способ системного представления деятельности на современном этапе развития методологических подходов к решению проблем ЗИ.

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

Определение 4. Окружение процесса – среда процесса, порождающая совокупность внутренних и внешних сил, которые способствуют или мешают достижению целей процесса (рис. 2).

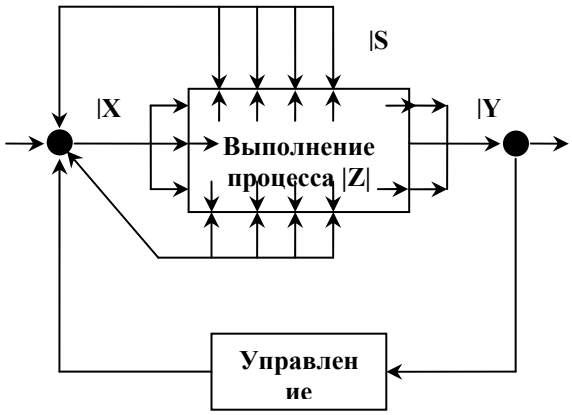


Рисунок 2 – Общая схема воздействия внешних и внутренних факторов на процесс $|X|$ – вектор начальных условий; $|Y|$ – вектор конечных условий; $|S|$ – вектор воздействий внешнего окружения; $|Z|$ – вектор факторов внутренней среды процесса

Факторы окружения процесса необходимо проанализировать и выделить из них те, которые могут оказать на выполнение процесса заметное влияние. Процесс нельзя отделять от 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 ЗИ.

Определение 5. Участники процесса ЗИ – 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 ЗИ заинтересован субъект ЗИ. С точки зрения процесса он выступает в роли *владельца процесса*.

Определение 6. Владелец процесса – это субъект, который осознал свои потребности в обеспечении безопасности информации и необходимость решения задач защиты, т. е. имеет потребности в конкретных результатах ЗИ, 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, поэтому 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 7. Выход процесса есть поток материальных или информационных объектов (продуктов), являющийся результатом выполнения процесса и потребляемый внешними по отношению к процессу объектами.

Выход процесса ЗИ 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 ЗИ могут относиться документация, информация, требования безопасности, новое состояние объекта информатизации и т. д.

Определение 8. Вход процесса ЗИ – это поток материальных или информационных объектов (продуктов), который в ходе выполнения процесса преобразуется в выход.

Определение 9. Ресурс процесса ЗИ – материальный или информационный объект, постоянно используемый для выполнения процесса, но не являющийся входом процесса.

К ресурсам процесса ЗИ 47 могут относиться: информация, персонал, оборудование, техника защиты, программное обеспечение, инфраструктура, среда, телекоммуникации и т. д.

Рассмотрим процесс как объект управления. 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 ЗИ 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 ЗИ [1] важно четко определить субъекты и объекты управления. Объектом управления является процесс ЗИ 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.

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 надо 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 осуществляется не сам по себе, а с целью выполнения каких-либо функций 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 ЗИ как субъекта управления.

Определение 10. Управляющий процессом ЗИ – это должностное лицо или коллегиальный орган управления, имеющий в своем распоряжении ресурсы, необходимые для выполнения процесса ЗИ и несущий ответственность за результаты процесса ЗИ перед владельцем процесса.

III Формальная модель процесса ЗИ

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

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

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 учитываются 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.

В основу предлагаемой формальной модели процесса положим следующие аксиоматические конструкции.

A1. Набор (множество) операций и действий $\mathbf{O} = \{o_1, o_2, \text{K } o_n\}$ по защите информации, составляющие процесса ЗИ P.

A2. Множество отношений $\mathbf{R} = \{r_1, r_2, \text{K } r_m\}$ 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.

A3. Цель Tar и ожидаемые результаты процесса Rez формируют назначение процесса

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

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

A4. Множество входов $IN = \{I^{in}, M^{in}\}$ и выходов $OUT = \{I^{out}, M^{out}\}$ 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 $\grave{I}$ представляет собой непрерывное или дискретное множество материальных объектов $\grave{I} = \{m_1, m_2, \text{K}, m_q\}$, распределенных во времени.

Информационный поток I представляет собой непрерывное или дискретное множество информационных объектов $I = \{i_1, i_2, \text{K}, i_q\}$. В соответствии с методологией IDEF0 выделяют ограничительную информацию $I^{îãð}$, описательную информацию $I^{îï}$ и управляющую информацию $I^{óïð}$.

Ограничительная информация $I^{îãð}$ представляет собой сведения запрещающего характера, которые содержатся 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 $I^{îï}$ представляет собой сведения об атрибутах объектов, которые подаются на вход и формируются на выходе процесса P и преобразуются 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 $I^{óïð}$ 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.

A5. Множество участников-субъектов процесса

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

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.

$$Process\_Team(PS, role, authority). \quad (4)$$

A6. Множество финансовых, временных, трудовых, материальных и иных ресурсов, необходимых для реализации и выполнения процесса P

$$Resource = \{Fin, T, Lab, Tan\}. \quad (5)$$

Введенные аксиоматические конструкции позволяют предложить формальную модель процесса

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

На рис. 3 представлена графическая интерпретация формальной модели. Данная модель может рассматриваться как базовая для дальнейших исследований.

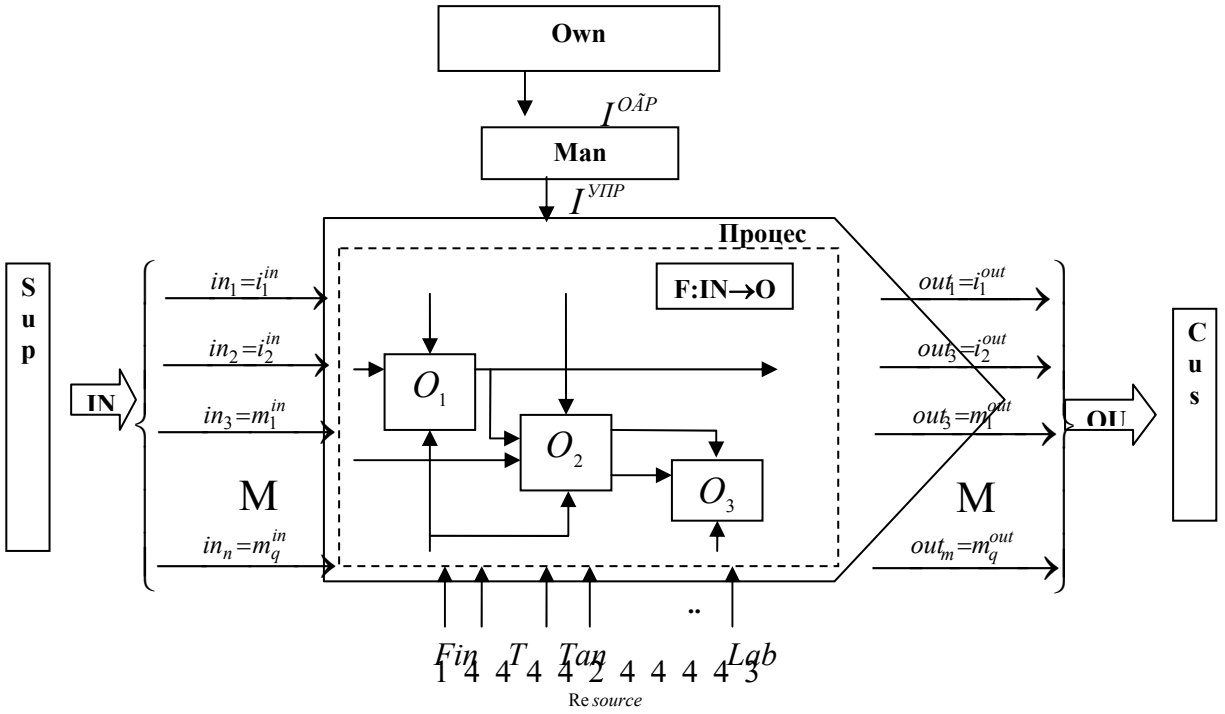


Рисунок 3 – Формальная модель процесса защиты информации

IV Эталонная модель системы процессов ЗИ

Изменение условий работы организаций и предприятий в условиях рынка, жестокой конкуренции выдвигает новые требования и к осуществлению деятельности по ЗИ. Работа службы ЗИ должна быть тщательно спланирована и стабильна, перемены в среде безопасности должны отслеживаться и контролироваться, ресурсы – эффективно использоваться и распределяться, уязвимости, сбои, последствия инцидентов безопасности – контролироваться и быстро устраняться, услуги безопасности – соответствовать уровню обязательств, потенциальные угрозы – предотвращаться, операции по ЗИ выполняться без перерывов и т. д. Очевиден следующий вывод: если деятельность службы ЗИ не организована, не взаимодействует с другими подразделениями и службами организации, то не будет обеспечено и качественное выполнение функций безопасности, невозможно будет обеспечить заданный уровень удовлетворенности (уверенности) владельца критической информации в ее безопасности. С таких позиций руководитель подразделения ЗИ должен задать себе ряд вопросов:

- какие процессы ЗИ необходимы для обеспечения требуемого уровня безопасности информации?
- какие отношения и связи между процессами ЗИ необходимы для обеспечения безопасности информации?
- какие технологии необходимы для запуска процесса ЗИ и обеспечения всесторонней интеграции мер ЗИ в повседневную деятельность?
- какие организационные структуры обеспечат эффективное выполнение процессов ЗИ и достижения целей безопасности?

Однако ответ на вопрос, «что» необходимо организации, тут же поднимает вопросы «как» и «где». Например:

- как разработать и реализовать процессы ЗИ, обеспечивающие требуемый уровень безопасности информации?
- как быстро и эффективно внедрить технологии, технику и средства ЗИ в повседневную практику?
- как определить, какие меры ЗИ (функции безопасности) следует реализовать собственными силами, а какие (если в этом есть потребность) – силами привлеченных со стороны специалистов?
- с чего начинать?

Рассмотренные выше аспекты убедительно говорят о необходимости разработки и использования системной модели процессов ЗИ в организации, поскольку руководителям организации, руководителям подразделений по ЗИ, офицерам безопасности необходима четкая картина деятельности по ЗИ. Без четкого представления процесса ЗИ организация столкнется с трудностями при определении:

- текущего состояния практической деятельности (работы) по ЗИ;
- желаемого состояния ЗИ в будущем;
- разрыва между текущем и желаемым состояниями;
- стратегии устранения этого разрыва.

Определение 11. Система процессов ЗИ – это совокупность взаимосвязанных и взаимодействующих процессов организации, включающих в себя все виды деятельности по ЗИ, которые могут выполняться в организации.

Можно выделить эталонную, нормативную и рабочую системы процессов ЗИ.

Эталонная система процессов ЗИ $S_Э$ – теоретически обоснованная непротиворечивая, полная совокупность процессов ЗИ, которые могут быть реализованы в организации.

Нормативная система процессов ЗИ S_H – совокупность процессов ЗИ, которые необходимо осуществлять в организации в соответствии с требованиями нормативных и иных документов.

Рабочая система процессов ЗИ S_P – совокупность процессов ЗИ, которая включает в себя все виды деятельности по ЗИ, которые осуществляются на данном предприятии (организации) в текущий плановый (анализируемый) период.

С точки зрения теоретико-множественного подхода для данных систем процессов справедливо соотношение

$$S_Ð \subseteq S_Í \subseteq S_Ý . \qquad (7)$$

В данной работе предлагается эталонная модель процессов ЗИ, которая получила название «дом процессов ЗИ». Предлагаемая модель представляет собой карту отношений высокоуровневых процессов ЗИ. Модель описывает процессы, которые организация может применять при осуществлении деятельности по ЗИ. Одним из назначений модели является предоставление общего базиса для различных моделей и методов аттестации процессов ЗИ и, в конечном итоге, оценки деятельности по ЗИ.

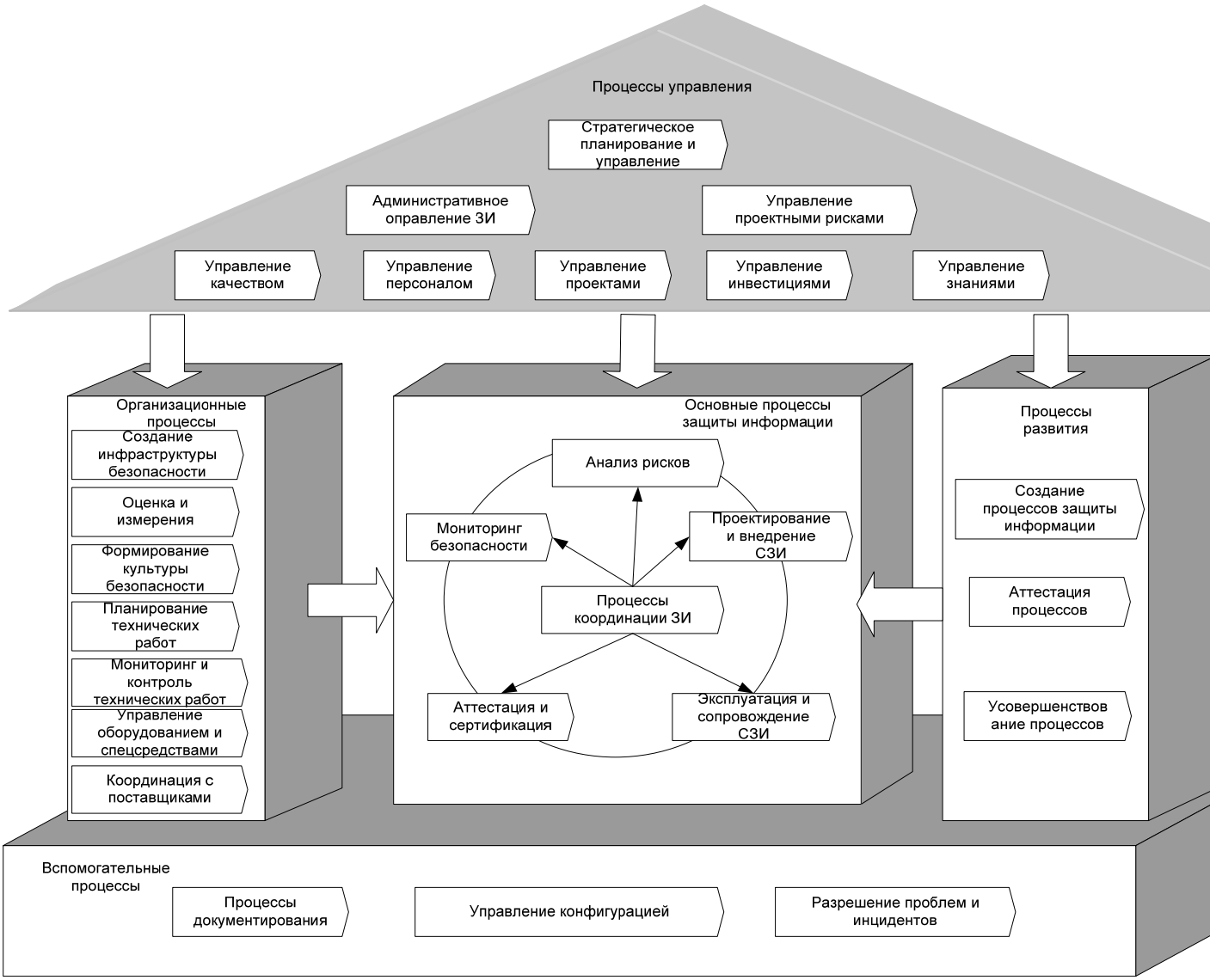
Модель может быть использована для:

- определения оценки текущего состояния деятельности по ЗИ;
- выявления недостатков в ЗИ и определения желаемого состояния деятельности по ЗИ в организации;
- определения приоритета при реализации мер ЗИ;
- определения критических связей между процессами;
- инициирования реорганизации процессов ЗИ в организации;
- определение сфер применения технологий ЗИ;
- определения возможностей реализации мер ЗИ внутренними силами и с помощью приглашенных специалистов.

Рассмотрим содержание предлагаемой модели. Одной из задач разработки эталонной модели является выделение и классификация процессов ЗИ. В основу процесса заложена необходимость реализации мер по ЗИ. При разработке классификации процессов ЗИ мы опирались в основном на действующие нормативные документы в области безопасности информационных технологий. Предлагается все процессы ЗИ разбить на пять классов. Каждый класс содержит процессы, имеющие общую целевую направленность и сосредоточены на определенном виде (направлении) деятельности, связанной с ЗИ. Такими классами являются:

- основные процессы ЗИ;
- процессы управления;
- организационные процессы;
- процессы развития;
- вспомогательные процессы.

На рис. 4 представлены отношения между этими группами процессов. Такое представление позволило автору предложить название эталонной модели процессов ЗИ – дом процессов ЗИ. Каждый класс может содержать в себе либо семейство процессов, либо непосредственно базовые процессы. Класс процессов, по сути, характеризует направление (вид) деятельности. Согласно [16], деятельность – это совокупность процессов, выполняемых (протекающих) последовательно или параллельно, преобразующих множество материальных или/и информационных потоков во множество материальных или/и информационных потоков. Семейство процессов характеризует субдеятельность, т. е. совокупность нескольких процессов в составе деятельности, объединенных некоторой частной целью. Семейство процессов состоит из базовых процессов. Базовый процесс является минимальным компонентом, который может быть включен в рабочую модель процессов ЗИ организации. Базовый процесс включает в себя операции и действия. Семейства выделяются только в классе основных процессов ЗИ для лучшей структуризации деятельности по ЗИ.


Процессы управления
Стратегическое планирование и управление
Административное оправление ЗИ
Управление проектными рисками
Управление качеством
Управление персоналом
Управление проектами
Управление инвестициями
Управление знаниями
Организационные процессы
Создание инфраструктуры безопасности
Оценка и измерения
Формирование культуры безопасности
Планирование технических работ
Мониторинг и контроль технических работ
Управление оборудованием и спецсредствами
Координация с поставщиками
Основные процессы защиты информации
Анализ рисков
Мониторинг безопасности
Проектирование и внедрение СЗИ
Процессы координации ЗИ
Аттестация и сертификация
Эксплуатация и сопровождение СЗИ
Процессы развития
Создание процессов защиты информации
Аттестация процессов
Усовершенствование процессов
Вспомогательные процессы
Процессы документирования
Управление конфигурацией
Разрешение проблем и инцидентов

Определение 12. Операция – это совокупность последовательно или/и параллельно выполняемых действий, преобразующих объекты, входящие в состав материального или/и информационного потока, в соответствующие объекты с другими свойствами. Операция выполняется: а) в соответствии с директивами, вырабатываемыми на основе директив, определяющих протекание процесса, в состав которого входит операция; б) с потреблением всех видов необходимых ресурсов; в) с соблюдением ограничений со стороны других операция и внешней среды. Учитывая предложенное определение процесса ЗИ (определение) и концептуальную модель (рис. 3) в основу определения операции закладывается та или иная мера ЗИ, которая должна быть предпринята [16].

Определение 13. Действие – преобразование какого-либо свойства материального или информационного объекта в другое свойство. Действие выполняется в соответствии с командой, являющейся частью директивы на выполнение операции, с потреблением необходимых ресурсов и соблюдением ограничений, налагаемых на осуществление операции [16].

При описании эталонной или нормативной модели декомпозиция осуществляется до уровня операций. Декомпозиция до уровня действий осуществляется при разработке рабочей модели.

Из-за ограниченного объема в данной статье рассматривается только перечень классов, семейств и базовых процессов, предлагаемых автором включить в состав эталонной модели процессов ЗИ. Данное множество разработано на основе анализа и с учетом требований: международного стандарта ISO/IEC 21847 (SSE-CMM) [20]; международного стандарта ISO/IEC 17799 [21]; международного стандарта ISO/IEC 13335 [22 – 24]; рекомендаций NIST SP 800-53 [25]; модели ИТ-процессов ITIL [26]; промышленного стандарта аудита информационных систем Cobit [27]; стандартной модели жизненного цикла систем ЗИSDLC [7].

Класс основных процессов ЗИ. Этот класс процессов определяет содержание деятельности по ЗИ и занимает центральное положение в эталонной модели. Процессы этого класса обеспечивают достижение главной цели и основных задач ЗИ в организации. Класс основных процессов ЗИ включает в себя следующие семейства процессов ЗИ:

1. семейство процессов анализа рисков безопасности, в состав которого входят: процесс анализа угроз безопасности информации, процесс оценки уязвимостей, процесс оценки ущерба, процесс оценки рисков безопасности, процесс категорирования информации;
2. семейство процессов проектирования и внедрения системы ЗИ, в состав которого входят: процесс планирования ЗИ; процесс определения потребностей в ЗИ; процесс определения технических решений по ЗИ;
3. семейство процессов эксплуатации и сопровождения системы ЗИ;
4. семейство процессов сертификации и аттестации ЗИ, в состав которого входят процессы аттестации и верификации системы ЗИ, процессы предоставления гарантий безопасности;
5. семейство процессов мониторинга безопасности, в состав которого входят процессы внутреннего аудита безопасности, процессы обеспечения независимого аудита безопасности, процессы мониторинга состояния ЗИ, процессы мониторинга процессов ЗИ;
6. процессы координации безопасности.

Класс процессов управления. Областью процессов управления является деятельность по управлению ЗИ и остальными видами деятельности, связанной с ЗИ. В данный класс входят процессы, содержащие операции и действия, которые могут быть использованы для управления проектами, процессами жизненного цикла ЗИ и т. д. Данный класс составляют такие процессы: процессы административного управления ЗИ, процессы стратегического управления ЗИ, процессы управления качеством ЗИ, процессы управления персоналом, процессы управления проектами, процессы управление инвестициями, процессы управления знаниями, процессы управления проектными рисками.

Класс организационных процессов. Класс организационных процессов включает в себя процессы, которые определяют цели организации в области ЗИ, создают активы и ресурсы для процессов ЗИ, которые при соответствующем использовании помогут организации достичь желаемой цели в области ЗИ. В данный класс входят процессы создания инфраструктуры безопасности, процессы оценки и измерения, процессы формирования культуры безопасности, процессы согласования требований безопасности, процессы планирование технических работ, процессы мониторинга и контроля технических работ, процессы управления оборудованием и специальными средствами, процессы координация с поставщиками.

Класс процессов развития охватывает деятельность по усовершенствованию процессов ЗИ, основной целью которой является определение, аттестация, измерение и оценка, контроль и улучшение процессов, относящихся к ЗИ. Данный класс состоит из процессов создания процессов ЗИ, процессов усовершенствования и процессов аттестации процессов обеспечения зрелости процессов ЗИ.

Класс вспомогательных процессов состоит из процессов, которые могут быть использованы любым другим процессом из других классов. К данному классу относятся процессы документирования, процессы управления конфигурацией, процессы разрешение проблем и инцидентов.

Заключение

Сегодня вопросы управления являются одними из актуальных вопросов в области ЗИ, что демонстрируется вниманием к этим вопросам в международных стандартах. Однако вопросам разработки научных и методических основ управлению ЗИ, к сожалению, уделяется недостаточное внимание. В данной статье впервые излагаются основы процессного подхода к управлению ЗИ, формулируется оригинальная концепция процессного подхода и раскрывается его сущность в рамках системодеятлельной методологии ЗИ.

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

Важным результатом является разработка информационной модели типа «сущность – отношение», которая раскрывает позицию автора относительно взаимосвязи между основополагающими категориями системодеятельной методологии ЗИ, а именно между категориями «ЗИ», «меры ЗИ» и «процесс ЗИ».

Для изучения свойств процесса, разработки различных моделей процесса (например, моделей зрелости, эффективности и т. п.), разработки системы процессов ЗИ в работе предлагается обобщенная формализованная 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 изучения такой категории, как процесс ЗИ.

Предложенная эталонная модель процессов ЗИ – дом процессов ЗИ, формирует системную и методическую основы для моделирования деятельности по ЗИ в рамках процессного подхода и раскрывает дальнейшие пути уточнения содержания ЗИ. Мы исходим из того, что процесс ЗИ, прежде всего, необходим для реализации мер по ЗИ. Именно с таких позиций в данной модели вводятся различные классы и семейства процессов ЗИ и определяются отношения между ними, которые не нашли своего отражения в существующих моделях деятельности по ЗИ (единственной системной моделью на сегодняшний день является модель SSE-CMM). Предлагаемая модель представляет собой карту отношений высокоуровневых процессов ЗИ. Модель описывает процессы, которые организация может применять при осуществлении деятельности по ЗИ. Одним из назначений модели является предоставление общего базиса для различных моделей и методов аттестации процессов ЗИ и, в конечном итоге, оценки деятельности по ЗИ.

Литература: ***1.*** *Потій О. В. Процесний підхід до управління безпекою інформації // VIII Международная научно-практическая конференция "Безопасность информации в ITC", 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. – 2003. – Вып. 134. – С. 9 – 25.* ***6.*** *Schwickert C, Fisher K. Der Geschaftsprozeb als formaler Prozeb – definition, eigenschafte und arten. Arbeitspiere 4, BWL, 1996.* ***7.*** *NIST SP 800-14. Generally Accepted Principles and Practices for Securing Information Technology Systems. M. Swanson, B. Guttman – 1996.* ***8.*** *NIST SP 800-27. Engineering Principles for Information Technology Security (A Baseline for Achieving Security). G. Stoneburner, C. Hayden, A. Feringa – 2004.* ***9.*** *ДСТУ ISO 9000-2001. Системи управління якістю. Основні положення та словник.* ***10.*** *Нортон Д., Каплан Р. Система сбалансированных показателей. От стратегии к действию. – М.:Олимп-Бизнес, Библиотека IBS, 2003.* ***11.*** *Деминг В. Едвард. Выход из кризиса. – Тверь: Альба. 1994.* ***12.*** *Martyn A. Ould. Business Process: Modeling and Analysis for Reengineering and Improvement. John Wiley&Sons, 1995.* ***13.*** *Otto K. Ferstl, Elmar J. Sinz. Busness Process Modeling. Wirtschaftsinformatik, Vol. 35 – 1993. – P.589-592.* ***14.*** *R. A*

Snowdon, B. C. Warboys. An Introduction to Process-Centered Environments. Software Process Modeling and Technology. RSP, 1994 - P 1 – 8. ***15.*** *Марка Д., Мак Гонэн К. Методология структурного анализа и проектирования - М.:МетаТехнология, 1993.* ***16.*** *РД IDEF 0. Методология функционального моделирования IDEF0. Руководящий документ. – Госстандарт России, Москва.- 2000.* ***17.*** *Каменова М., Громов А., Ферапонтов М., Шматлюк А. Моделирование бизнеса. Методология ARIS. – М.: ООО «Издательство Серебряные нити», 2001. – 327 с.* ***18.*** *Шеер А. В. Бизнес-процессы. Основные понятия. Теория. Методы. – М.: Вестъ-МетаТехнология, 1999.* ***19.*** *Шеер А. В. Моделирование бизнес-процессов. - М.: Вестъ-МетаТехнология, 2000.* ***20.*** *ISO/IEC 21827: 2002. Information technology - Systems Security Engineering - Capability Maturity Model.* ***21.*** *ISO/IEC 17779:2000. Code of practice for information security management.* ***22.*** *ДСТУ ISO/IEC TR 13335-1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1: Концепції та моделі безпеки інформаційних технологій.* ***23.*** *ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій.* ***24.*** *ДСТУ ISO/IEC TR 13335-3:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3: Методи керування безпекою інформаційних технологій.* ***25.*** *NIST SP 800-53. Recommended Security Controls for Federal Information Systems. R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, G. Rogers, A. Lee. – 2005.* ***26.*** *ITIL IT Management Practices: Information Technology Infrastructure Library. Practices and guidelines developed by Central Computer and Telecommunications Agency (CCTA), London, 1995.* ***27.*** *Control Objective for Information and related Technology (CobiT). IT Governance Institute,ISACA/-2000.*

УДК 681.3.06

МЕТОДИКА ОЦІНКИ ВІДПОВІДНОСТІ ПОТОЧНОЇ ЗРІЛОСТІ ЦІЛЬОВИМ ОРІЄНТИРАМ

Олександр Потій, Анатолій Лєншин
ЗАТ „Інститут інформаційних технологій”

Анотація: **Пропонується методика оцінки зрілості процесів захисту інформації, особливістю якої є формалізована оцінка відповідності поточної зрілості цільовим орієнтирам.**
Summary: **The evaluation methods of security process maturity that includes formal compliance assessment of current and target maturity are proposed.**
Ключові слова: **Захист інформації, зрілість процесів, експертні оцінки.**

Вступ

Одним із найважливіших моментів проведення оцінки зрілості процесів захисту інформації (ПЗІ) є прийняття рішень на основі зібраних даних та отриманих експертних оцінок. Сутність прийняття рішення на фінальній стадії полягає в розв’язанні таких задач:

- сформувати оцінку поточної зрілості процесів захисту інформації;
- визначити ступінь відповідності цільових орієнтирів та отриманих результатів оцінки зрілості процесів захисту інформації;
- визначити перелік та черговість ПЗІ, зрілість яких необхідно підвищити негайно, які потребують покращення, але при цьому не є критичними для бізнес цілей організації;
- визначити типові недоліки, притаманні системі управління зрілістю ПЗІ в цілому, та сформувати поради щодо їх усунення;
- порівняти якість здійснення заходів з підвищення зрілості на кількох об’єктах.

Основною проблемою при вирішенні цих задач є відсутність науково-методичного апарату оцінки зрілості ПЗІ, що забезпечує об’єктивність, порівнянність та повторюваність результатів оцінки, та дозволяє формувати рекомендації щодо поліпшення (вдосконалення) ПЗІ та захисту інформації в цілому. Великий обсяг вхідних та вихідних даних, необхідність здійснення рутинної роботи поряд з необхідністю прийняття рішень з одного боку та відсутність науково-методичного апарату з іншого – загострюють проблему автоматизації процесу оцінки зрілості ПЗІ в цілому, зокрема в частині прийняття рішень.

І Етапи та задачі оцінки зрілості ПЗІ

Сутність задачі оцінки зрілості ПЗІ полягає в тому, щоб у конкретний момент часу з використанням