- обґрунтовано вибір методу трансформації вихідного зображення;
- обґрунтовано вибір методу кодування квантованих трансформант зображення;
- розроблено структурну модель процедури стиснення зображень з урахуванням методу кодування за кількістю бітових переходів.

ЛІТЕРАТУРА

1. Юдін. О.К. Методи структурного кодування даних в автоматизованих системах управління / О.К. Юдін – К.: НАУ, 2007.
2. Юдін О.К. Використання аналітичних перетворень в задачах стиснення зображень / К.О. Курінь, О.К. Юдін, О.І. Варченко // Наукоємні технології. – К.: Вид–во Нац. авіац. ун–ту «НАУ–друк», 2011. – № 13(7). – С. 64–69.
3. Воробьев В.И. Теория и практика вейвлет-преобразования / В.И. Воробьев, В.Г. Грибунин. – СПб.: ВУС, 1999. – 203 с.
4. Селомон Д. Сжатие данных, изображений и звука / Д. Селомон – М.: Техносфера, 2006. – 386с.
5. Юдін О.К. Метод кодування двійкових послідовностей за кількістю бітових переходів / О.К. Юдін, К.О. Курінь // Наукоємні технології. – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2010. – №3 (15). – С. 87-92.

Надійшла: 10.10.2012 р.

Рецензент: д.т.н., професор Давлет'янц О.І.

УДК 004.056

Архипов А.Е.

ОСОБЕННОСТИ АНАЛИЗА РИСКОВ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

В статье рассмотрены основные свойства информационно-коммуникационных систем (ИКС), дано определение термина ИКС, обоснована необходимость процессного задания вероятностных свойств реализаций угроз информации в ИКС и введения динамических характеристик рисков угроз. Рассмотрены сценарные и экспертные способы задания терминальных вероятностей угроз.

Ключевые слова: информационно-коммуникационная система (ИКС), коммуникационная система, коммуникационная технология, терминальная вероятность, динамический риск, сценарии угроз.

Вступление

Относительно недавно появившееся в журнальных публикациях словосочетание «информационно-коммуникационные системы» (ИКС) достаточно быстро стало привычным в сфере технической защиты информации. При этом очень часто аббревиатура ИКС просто механически заменяет широко использовавшуюся ранее аббревиатуру ИТС – информационно-телекоммуникационная система, что по умолчанию предполагает полную синонимичность (или эквивалентность) терминов ИКС и ИТС. Однако если содержание термина ИТС достаточно четко изложено в нормативно-правовых документах [1,2], то ситуация с ИКС диаметрально противоположна. Поэтому прежде чем приступить к рассмотрению рисков в ИКС, попытаемся уточнить ее основные свойства и характеристики.

Чаще всего появление термина «информационно-коммуникационные системы» (ИКС) связывают с введением в вузах Украины подготовки бакалавров по программе 6.170101 «Безопасность информационных и коммуникационных систем» в области знаний 1701 «Информационная безопасность». Однако термин «ИКС» использовался и раньше, в частности, в [3] ИКС представляется как эффективное средство управления в сфере предпринимательства и обеспечения безопасности организации. К сожалению, в отечественных нормативно-правовых документах определение термина ИКС отсутствует. Это влечет возможность неоднозначной трактовки данного понятия, порождая ряд негативных последствий, в частности, противоречия в категориально-понятийном аппарате защиты информации, что является абсолютно недопустимым как в этой, так и в любой другой сфере деятельности. Поэтому прежде чем приступить к рассмотрению рисков в ИКС, следует сформулировать содержание самого термина ИКС.

Авторы уже упоминавшегося выше учебного пособия [3] определяют ИКС как автоматизированную систему управления (АСУ), упорядочивающую и контролирующую информационные потоки в организации, снабжающую необходимой информацией ее структурные подразделения, обеспечивающую своевременную подготовку и принятие решений, дополненную эффективной системой межличностных коммуникаций на всех уровнях и во всех подразделениях организации, что в конечном счете обеспечивает успешное решение как производственных, так и управленческих задач.

Важность процессов коммуникации для реализации управленческих функций подчеркивается во многих учебных пособиях по теории организаций, информационным технологиям управления и менеджмента [4-8]. Однако большинство из них ограничивается исследованием ситуации на уровне анализа и оценки влияния межличностных коммуникаций на степень успешности менеджмента и управления, избегая исследования этой проблемы в условиях комплексного применения ИС и процессов коммуникации.

Следует отметить, что термин ИКС определен в российской нормативной базе. Согласно введеному в июле 2008 года стандарту ГОСТ Р 52653-2006 – *Информационно-коммуникационные технологии в образовании. Термины и определения*, ИКС – «совокупность инженерного оборудования, предназначенного для комплексного управления технологическими процессами в зданиях и сооружениях образовательных учреждений с применением средств вычислительной техники и телекоммуникаций». В данной дефиниции ИКС специфицируктся исключительно как ИС, а именно, АСУ технологическими процессами в образовательной сфере, при этом совершенно игнорируется наличие второй составляющей ИКС – коммуникационной системы. Поэтому особенный интерес при рассмотрении понятия ИКС представляют два аспекта: содержание понятия «коммуникационная система» (КС), взаимодействие ИС и КС в процессе функционирования ИКС.

ИКС – новое направление развития ИС

В шестидесятых годах прошлого века широкое развитие получили автоматизированные системы управления производством (АСУП), одним из элементов которых являлись автоматизированные системы управления технологическими процессами (АСУ ТП). Если вначале понятие технологического процесса соотносилось с совокупностью операций по переработке физического сырья и полуфабрикатов в готовую продукцию, то несколько позже оно было расширено на процессы, в которых и исходные материалы, и конечный продукт представляли собой информацию [8,9]. Иногда в специальной литературе для подобных процессов вводится особое определение: алгоритмические процессы (АП) [9].

Основные области применения АСУ ТП(АП) – автоматизация рутинных вычислительных работ, типовых расчетов, централизованное решению ряда функциональных задач в сфере экономики, снабжения, учета, планирования, и т.п. Типичная «традиционная» АСУ ТП(АП) – замкнутая информационная система (ИС), обеспечивающая в соответствие с жестко заданным алгоритмом сбор, транспортировку (передачу) и обработку информации с последующим формированием и реализацией управляющего воздействия, необходимого для оптимизации управления технологическим объектом. Подобные ИС широко применяются в крупносерийном централизованном производстве с четко очерченными функциями подразделений, с достаточно устойчивой и консервативной номенклатурой производимых конечных продуктов.

Помимо АСУ ТП(АП), широкое распространение получили ИС управления организационно-технологическими процессами предприятия (АСУП) и ИС организационного управления. Однако характерная для начальных этапов развития АСУ жесткая функциональность и централизация процессов управления, обусловившие в конечном счете иерархичность структур управления, оказались неэффективными в ряде сфер деятельности. В первую очередь это касается венчурных предприятий, выполняющих форвардные наукоемкие проекты, производителей уникальных или малосерийных продуктов, управленческих подразделений, решающих задачи экономического и финансового менеджмента, различных структур, осуществляющих аналитическое

сопровождение и информационную поддержку менеджмента. Для таких организаций их основной производственной и организационно-управленческой моделью стал бизнес-процесс – целенаправленная динамическая структура, представляющая собой упорядоченную совокупность действий (бизнес-процедур), в результате выполнения которых создается некоторый продукт (или реализуется определенная услуга). Структура бизнес-процесса не постоянна и формируется сообразно конкретным заданиям (заказам), с целью выполнения которых и организуется бизнес-процесс, причем отдельные элементы этой структуры функционируют лишь в течение конечного промежутка времени, необходимого для реализации соответствующих бизнес-процедур.

Отличительной чертой бизнес-процессов является доминирование в них информационных бизнес-процедур, реализуемых системами информационных технологий. Прототипом подобных систем можно считать информационную систему офиса, прошедшую в своем развитии несколько стадий [8]. Первоначально в ИС офиса решались задачи формирования и распределения информационных потоков внутри организации, в частности, вопросы, связанные с накоплением и хранением информации, обеспечением ее обмена между исполнителями, обеспечением поиска релевантной информации, а также вопросы координации, оптимизации и контроля выполнения работы исполнителями, принятия производственных и административно организационных решений определенного уровня. Поэтому к офисным ИС в той или иной степени можно отнести финансово-экономические, бухгалтерские и аналитико-информационные подразделения, отделы сбыта, рекламы, конструкторские бюро, банки, консалтинговые фирмы, страховые компании, налоговые службы, системы менеджмента и управленческие структуры. Для работников большинства перечисленных подразделений и структур характерна необходимость принятия решений, носящих интуитивно-субъективный характер, что обуславливает высокий уровень эмоциональных и психологических перегрузок.

Предположения специалистов в области информатики о возможности предупреждения этих перегрузок путем создания и широкого применения разного рода экспертных систем (ЭС) и систем поддержки принятия решений (СППР) оказались не оправдано оптимистичными: процедура формализации совокупности получаемых от эксперта сведений, «закачиваемых» в базу знаний ЭС или СППР, приводит к выхолащиванию из этих сведений так называемых «знаний второго рода» [10] - интуитивных знаний, составляющих до 80% неформальных знаний экспертного сообщества [11]. Поэтому особую важность приобретает наличие внутренних и внешних связей и деловые коммуникаций сотрудников офиса, готовность и умение работать в «команде» - сетевой коммуникативной структуре, аккумулирующей неформальные знания в различных сферах профессиональной деятельности. Таким образом, потребность в развитой системе коммуникаций – необходимое условие успешного менеджмента бизнес-процессов.

Отметим, что в отличие от ИКС термин «коммуникация» определен в украинской нормативной базе: коммуникация – взаимосвязь субъектов с целью передачи информации, согласования действий, совместной деятельности [11]. Там же [11] описаны возможные способы и формы коммуникаций, характеристики степени их интенсивности и глубины, например (ниже приведены некоторые фрагменты спецификаций коммуникации, перечисляемые по мере роста степени ее интенсивности и глубины):

- ситуативное взаимодействие в ограниченном круге лиц с помощью посторонних;
  …;
- способность к эффективной работе в команде, восприятие критики, советов и указаний, продуцирование устных и письменных сообщений, в частности в профессиональной сфере;
  …;
- доведение до специалистов и неспециалистов информации, идей, проблем, решений и собственного опыта в сфере профессиональной деятельности, умение эффективно формировать коммуникационную стратегию;
  …;
- лидерство, свободное компетентное общение в определенной сфере научной и / или профессиональной деятельности с широким кругом специалистов, в частности наивысшей квалификации, с общественностью.

Эффективная коллективная коммуникация характеризуется явным синергетическим эффектом, выражающемся в резком нелинейном "всплеске" интеллектуального потенциала "команды" и, как следствие, возможном получении нетривиальных прорывных решений в сфере профессиональной деятельности.

Проблема коммуникаций не ограничивается только сферой межличностного общения специалистов. Современные распределенные ИС состоят из большого числа отдельных разнородных приложений, в общем случае представляющих композицию гетерогенных компонентов. Эффективное взаимодействие между компонентами таких ИС реализуется с помощью специальных коммуникационных технологий, обеспечивающих:

- межязыковую коммуникацию (можно вызвать функцию, написанную на одном языке программирования, из кода, написанного на другом языке);
- обработку данных, изначально представленных в разных форматах;
- прямую и обратную совместимость программного обеспечения и данных: старые версии программного обеспечения могут обрабатывать данные, пришедшие от новых версий и наоборот;
- независимую конвертацию данных из одного формата в другой;
- совместимость со сторонним программным обеспечением и др.

Очевидно, что любую коммуникацию можно рассматривать как результат реализации набора соответствующих коммуникационных технологий, которые допускают изучение, описание и спецификацию [12-14]. Совокупность коммуникационных технологий, характеризующуюся определенной структурой и применяемую для обеспечения того или иного вида практической деятельности, назовем коммуникационной системой (КС). Тогда ИКС можно определить как комплекс информационной и коммуникационной систем, которые в процессе их функционирования действуют как единое целое. Цель ИКС – реализация технологий обработки информации при максимально полной активации потенциальных возможностей элементов, входящих в состав структуры системы, в частности, усиление интеллектуального потенциала коллектива обработчиков путем вовлечение индивидуальных неформальных знаний в процесс обработки, создание условий для полноценного и эффективного функционального взаимодействия разнородных компонентов распределенной ИС.

Терминальные вероятности и динамические риски в ИКС

Если для традиционных АСУ, в частности АСУ ТП, стабильность состава производственных операций, неизменность требований к характеристикам выпускаемой продукции, относительная стабильность условий среды функционирования влекут за собой постоянство модели угроз и, как следствие, создание достаточно консервативной по своим параметрам системы защиты информации, то ситуация с защитой информационных ресурсов бизнес-процессов диаметрально противоположная. Особенностью бизнес-процесса является конечный цикл реализации отдельных бизнес-процедур, в ходе выполнения которых применяются различные системы информационных технологий с присущими им индивидуальными особенностями, в том числе и уязвимостями по отношению к угрозам информации. Поэтому структура модели угроз бизнес-процесса является динамической, ее отличительные особенности:

- непостоянство состава модели угроз бизнес-процесса, ее зависимость от конкретики решаемой задачи (выполняемого задания, оказываемой услуги);
- конечное время существования включенных в модель угроз (как правило, связанное с развитием бизнес-процесса, портфелем заказов, их продолжительностью);
- распределение вероятности каждой из угроз в пределах промежутка времени τ, соответствующего времени существования угрозы.

Последняя особенность обусловила введение в рассмотрение так называемой терминальной вероятности реализации угрозы $P(t)$, которая распределена на интервале времени τ по определенному закону [15]:

$$P(t) = P_m \int_0^t p(t)dt = P_m \int_{t_1}^{t_1+t} p(t)dt \qquad (1)$$

и соответствует значению вероятности реализации угрозы $P(t)$ за определенный промежуток времени $t \le \tau$, прошедший с момента начала реализации угрозы (*терминальная* от латинского *terminus* – предел, срок, определенное время), причем $\int_0^\tau p(t)dt = 1$, а значит $P(\tau) = P_m$. При задании терминальной вероятности $P(t)$ в качестве функции плотности распределения $p(t)$ могут быть использованы как типовые виды распределений вероятностей, так и специфические, формы которых определяются конкретными особенностями ситуаций, возникающих в ходе развития событий в системе "атака-защита". Пример изменения терминальной вероятности $P(t)$ во времени приведен на рис.1.

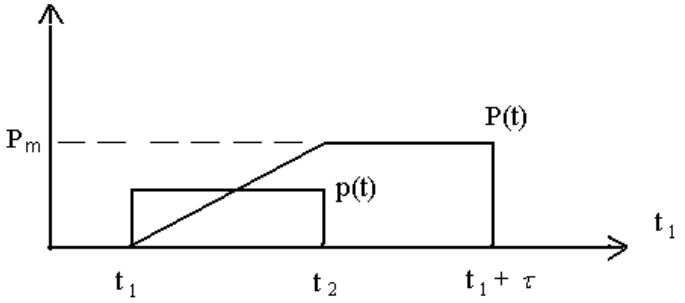

Рис.1. Терминальная вероятность: зависимость значения вероятности $P(t)$ от плотности распределения $p(t)$ и времени τ существования угрозы

Момент возникновения угрозы – t_1, время ее существования – τ, $p(t)$ – плотность терминальной вероятности, равномерно распределенная во временном промежутке $[t_1, t_2]$, что обуславливает линейный рост в этом же промежутке терминальной вероятности $P(t)$ от 0 до ее максимального значения P_m с последующим сохранением своего значения до момента $t_1 + \tau$ завершения бизнес-процесса. В момент $t_1 + \tau$ вероятность скачком спадает до 0. Это можно интерпретировать как мгновенное полное исчезновение у атакующей стороны интереса к информации, являющейся объектом атак. Примером подобной ситуации может быть проведение конкурса на лучшее решение некоторой задачи (проблемы) в условиях полной конфиденциальности проектов и их авторов. Полуинтервал $[t_1, t_2)$ соответствует сбору заявок на участие в конкурсе, подаче проектов, интервал $(t_2, t_1 + \tau)$ – обсуждению поданных проектов, момент времени $t_1 + \tau$ – объявлению результатов конкурса.

Использование терминальных вероятностей позволяет учесть динамику развития атак, обычно остающуюся "за кадром" при традиционном подходе к анализу угроз. Рассмотрим предполагаемый сценарий развития некоторой угрозы, осуществляемой посредством проведения трех независимых атак a1, a2, a3, характеризующихся вероятностями реализации P_1, P_2, P_3. Учитывая, что атаки независимы, но совместимы и могут осуществляться как поодиночке, так и в комплексе: < a1, a2>, < a2, a3>, ... , < a1, a2, a3>, можно сформировать из них полную группу событий, рассчитать вероятности этих событий, найти частные риски от реализации всех возможных атак (в том числе комплексных) и оценить для полной группы событий интегрированный информационный риск [16-17], характеризующий уровень защищенности информации. Выполненный анализ рисков позволяет выявить наиболее опасные атаки, комплексы атак и оптимизировать процесс защиты информации. Однако в этом анализе не учтен временный фактор, отражающий обязательное существование интервалов времени, необходимых для развития и реализации каждой из атак. При этом вероятности P_1, P_2, P_3, воспринимаемые обычно как ”точечные”,

на деле оказываются распределенными каждая внутри своего интервала. Особенности соответствующих распределений и продолжительности интервалов могут весьма существенно влиять на построение и реализацию плана защиты.

В частности, каждой атаке a_i, $i=\overline{1,3}$, можно поставить в соответствие вероятность $P_i(t)$, которая характеризует динамику проведения соответствующей атаки (рис.2), описываемую выражением $P_i(t)=P_i\int_0^t p_i(t)dt$, где P_i – исходная "точечная" вероятность, $P_i=P_i(\infty)$.

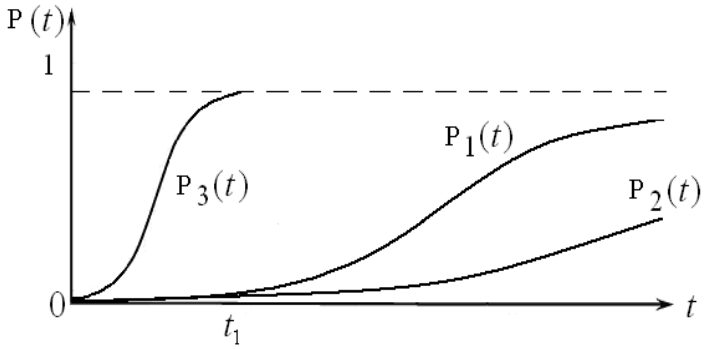

Рис.2. Изменение во времени терминальных вероятностей $P_i(t)$, характеризующих динамику развития атак

Очевидно, что для конкретной атаки успех ее проведения будет определяться степенью завершенности атаки, т.е. продолжительностью срока её развития и видом плотности вероятности $p_i(t)$ (рис.2). В рассматриваемом примере, если предположить, что $P_1 \approx P_2 \approx P_3$, терминальная вероятность $P_3(t)$ для малых значений t может оказаться значительно выше аналогичных вероятностей двух других атак. В частности, т.к. для t_1 справедливо соотношение: $P_3(t_1) >> P_1(t_1) > P_2(t_1)$, стратегия управления защитой окажется существенно отличной от той, которая вытекает из формального анализа рисков (т.е. без учета терминальных вероятностей, только с привлечением "точечных" вероятностей P_1, P_2, P_3).

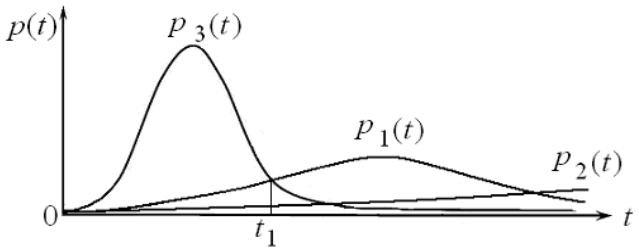

Рис.3. Распределение плотностей вероятностей $P_i(t)$

Приведенный выше пример позволяет предположить недостаточную корректность традиционной процедуры выделения существенных угроз (атак), сводящейся к ранжированию рисков соответствующих угроз (атак) и сопоставлению их с фиксированным пороговым уровнем, равным минимально допустимому значению риска. Вычисляемые риски в этой процедуре базируются на "точечных" вероятностях, тогда как объективность результатов ранжирования и попарного сопоставления с порогом может быть обеспечена только в случае применения терминальных вероятностей, рассчитанных для конкретного момента времени и учитывающих фактическую распределенность "точечных" вероятностей в пределах интервала времени проведения атаки.

В общем случае величина терминальной вероятности монотонно возрастает с увеличением значений времени *t*, однако особенности и темпы этого роста определяются исключительно формой зависимости *P(t),* учитывающей динамику нарастания степени обеспечения комплекса условий, гарантирующих успешное осуществление атаки. В качестве модельных распределений вероятности *P(t)* можно использовать традиционные виды распределений, представленных типовыми законами: равномерным, нормальным, лапласовым и т.п. При этом данные распределения будут смещены вправо, в сторону роста *t,* и усеченными слева для всех $t < 0$.

Очевидно, что если вероятности реализации угроз информации в ИКС характеризуются изменяющимися во времени величинами (терминальными вероятностями) то и значения рисков ИКС, обусловленных существованием этих угроз, не могут быть постоянными во времени. Следовательно, также как и вероятности, риски ИКС имеют принципиально динамический, процессный характер. При этом не исключено, что и второй компонент риска – ущерб (потери), обусловленный реализацией угрозы, тоже изменяется во времени. В общем случае все это ведет к существенному усложнению анализа риска. Поэтому если допустить, пусть в самом грубом приближении, возможность принятия гипотезы постоянства потерь, основная сложность анализа рисков будет сопряжена с нахождением оценок терминальных вероятностей. В связи с этим ниже остановимся исключительно на вопросах оценивания значений терминальной вероятности.

Сценарный способ задания терминальных вероятностей

Часто интерес представляет более детальное описание интервальной вероятности, выделение в ней отдельных составляющих, имеющих самостоятельное смысловое содержание, связанное с особенностями либо этапами реализации угроз.

Рассмотрим несколько вариантов (сценариев) развития подобных событий.

В ряде случаев вероятность реализации угрозы определяется по так называемой трехфакторной формуле [20]:

$$P(t) = P_T(t) P_V(t), \tag{2}$$

где $P_T(t)-$ вероятность возникновения угрозы, $P_V(t)-$ вероятность реализации атаки, ведущая к осуществлению угрозы.

Рассмотрим ситуацию, возникающую при реализации атакующей стороной А (злоумышленниками) угрозы *T* относительно некоторой информации (информационного ресурса) *I*, принадлежащего стороне В. Полагаем, что *D* – общая стоимость затрат атакующей стороны А на реализацию угрозы *T*, *g* – полученный при этом стороной А «выигрыш», определяемый ценностью информации *I* для злоумышленников [18,19].

Приведенные данные дают стоимостную характеристику ситуации «атака-защита». Требуется на базе этих сведений построить логико-эвристическую схему экспертного оценивания вероятностных характеристик, используемых для вычисления информационных рисков.

Очевидно, что активность стороны А в реализации угрозы *T* определяется в общем случае величиной чистой прибыли, которую сторона А может получить в случае успешной реализации угрозы *T*. Чем больше прибыль, тем устойчивее стремление стороны А к осуществлению угрозы *T*, которое количественно можно оценить вероятностью возникновения (активации) угрозы

$$P_T = \frac{g - D}{g} = 1 - \frac{D}{g}. \tag{3}$$

Предположим, что величина суммарных затрат *D*, понесенных атакующей стороной А на подготовку, организацию и проведение атакующих действий, является функцией времени. Тогда вероятность P_T также будет зависеть от времени, т.е. ее следует

рассматривать как терминальную вероятность $P_T(t)$. Если в некоторый момент времени $t_{\max}$ величина суммарных затрат $D(t_{\max})$ достигнет значения, при котором $D(t_{\max})/g$ станет равным 1, то в соответствии с формулой (2) терминальная вероятность $P_T(t_{\max})$ окажется равной 0, т.е. дальнейшее продолжение атакующих действий стороной А представляется нерациональным. Затраты $D(t_{\max}) = D_{\max}$ назовем предельно возможными затратами стороны А. Предположим далее, что текущие затраты δ атакующей стороны в среднем неизменны во времени. Тогда справедливы соотношения:

$$D(t) = \delta t \le D_{\max},\ t_{\max} = D_{\max}/\delta, \tag{4}$$

где $t_{\max}$ – длительность интервала времени, в течение которого сторона А полностью расходует свой атакующий ресурс и прекращает попытки реализации угрозы T по отношению к информации I, владельцем которой является сторона В.

Значение терминальной вероятности $P_T(t)$ в соответствие с выражениями (3), (4) определяется формулой:

$$P_T(t) = (1 - \frac{\delta}{g}t). \tag{5}$$

Кроме того будем полагать, что с ростом общего времени t, которое сторона А тратит на организацию, подготовку и проведение атак (т.е. по мере накопления стороной А опыта реализации угрозы и сведений о системе ЗИ стороны В), растет терминальная вероятность $P_v(t)$ успешного использования стороной А уязвимости V: $PV(t)=p_vt$, где p_v=const, т.е. плотность вероятности $p_v(t)$ распределена равномерно в промежутке $(0,\ t_v)$, $t_v > t_{\max}$. Тогда вероятность реализация угрозы T определяется выражением:

$$P(t) = P_T(t)P_V(t) = (1 - \frac{\delta}{g}t)p_vt = p_vt - \frac{\delta p_v}{g}t^2. \tag{6}$$

При этом вероятность $P(t)$ возрастает, начиная от $P(0)=0$ до своего максимального значения $P(t_{extr}) = 0{,}25 p_V g/\delta$, соответствующего моменту времени $t_{extr} = g/2\delta$, уменьшаясь затем вновь до 0: $P(t_{\max})=0$.

Возможен вариант сценария развития событий в системе "атака-защита", при котором доминирующим является влияние фактора времени на мотивацию и действия атакующей стороны А. В частности, предположим, что доступ к информации I возможен только в течение ограниченного полуинтервала времени $(0,\ t_m]$, т.е. $P(t)=0$ при $t > t_m$. В этой ситуации мотивация атакующей стороны А резко возрастает по мере приближения момента t_m (если ранее предпринимаемые атаки окончились неудачей), что отображается моделью вида:

$$P_T(t) = \frac{P_{Tm}}{t_m - t + 1},\ P_{Tm} = P_T(t_m). \tag{7}$$

Будем также полагать, что предположения относительно характера и особенностей изменения во времени интервальной характеристики P_V остались прежними, т.е. $P_V(t)=p_vt$. Тогда

$$P(t) = P_T(t)P_V(t) = \frac{P_{Tm}}{t_m - t + 1}p_vt. \tag{8}$$

Подобный сценарий характерен для развития событий, связанных с принятием стороной В некоторого критически важного для атакующей стороны А решения, заблаговременная информация о содержании которого жизненно важна для стороны А, в связи с чем затраты, обусловленные реализацией угрозы, отходят на второй план.

Особенности экспертного задания терминальных вероятностей. Байесовские оценки терминальной вероятности

Если продуцирование правдоподобных сценариев по какой – либо причине оказывается невозможным, выходом является экспертное задание значений терминальной

вероятности. Крайне высокий уровень субъективизма в экспертных оценках требует обязательного учета любых доступных достоверных сведений, позволяющих повысить надежность результатов, получаемых при обработке информации. Особенно важным это оказывается при определении терминальной вероятности, процедура оценивания которой должна обеспечить постоянное обновление значений вероятности. Эффективный способ задания подобной процедуры может основываться на теореме Байеса, применение которой позволяет реализовать механизм согласования ранее найденных и вновь поступивших данных о значениях терминальной вероятности, интегрируя в новых оценках вероятности весьма приближенные или даже противоречивые сведения.

Предположим, что при анализе угроз информации в ИКС выявлена некоторая угроза *T*, которая может быть осуществлена посредством двух отличных друг от друга атакующих действий. Первоначально определенная априорная вероятность успеха атаки А – p_a, атаки В – p_b. Анализ вновь поступившей оперативной информации свидетельствует об изменении значений исходных вероятностей, но при этом возникают две взаимоисключающие версии. По одной из них, степень правдоподобия которой оценивается как p_1, в ближайшей перспективе будет реализована атака А, по другой – атака В (степень правдоподобия этой версии оценивается как p_2).

Исходная ситуация, сложившаяся первоначально с реализацией угрозы *T*, предполагает существование четырех гипотез, составляющих полную группу событий:

H_1 = < реализация только атаки А >, $P(H_1) = p_a(1-p_b)$;

H_2 = < реализация только атаки В >, $P(H_2) = (1-p_a)p_b$;

H_3 = < реализация обеих атак А, В >, $P(H_3) = p_a p_b$;

H_4 = < не состоявшиеся попытки реализации обеих атак >, $P(H_4) = (1-p_a)(1-p_b)$.

Событие Е, состоящее в поступлении новой информации о возможности осуществления атак А, В, изменяет вероятности гипотез $H_1 - H_4$. Для их определения рассмотрим условные вероятности реализации события Е совместно с каждой из введенных выше гипотез:

$P(E / H_1)$ = < вероятность того, что вновь полученная информация правдива относительно реализация атаки А, но ошибочна относительно атаки В > $= p_1(1-p_2)$;

$P(E / H_2)$ = < вероятность того, что вновь полученная информация правдива относительно реализация атаки В, но ошибочна относительно атаки А > $= (1-p_1)p_2$;

$P(E / H_3)$ = < вероятность того, что вновь полученная информация правдива относительно реализация обеих атак А и В > $= p_1 p_2$;

$P(E / H_4)$ = < вероятность того, что вновь полученная информация ошибочна относительно реализация обеих атак А и В > $= (1-p_1)(1-p_2)$.

Приведенные выше условные вероятности позволяют рассчитать вероятность события Е. В соответствие с формулой полной вероятности получаем:

$$P(E) = \sum_{i=1}^{4} P(H_i, E) = \sum_{i=1}^{4} P(H_i)P(E/H_i). \quad (9)$$

Теперь можно по формуле Байеса определить условные вероятности гипотез $H_1 - H_4$ после получения дополнительной информации (событие Е):

$$P(H_i / E) = P(H_i)P(E / H_i) / P(E),\ i = \overline{1,4}. \quad (10)$$

В частности, если исходные данные принимают следующие значения: p_a =0,5, p_b=0,4, p_1=0,6, p_2=0,8, получаем: $P(H_1) = 0{,}3$, $P(H_2) = 0{,}2$, $P(H_3) = 0{,}2$, $P(H_4) = 0{,}3$, $P(H_1 / E) =$ 0,165, $P(H_2 / E) = 0{,}291$, $P(H_3 / E) = 0{,}436$, $P(H_4 / E) = 0{,}109$. Как видим, априорные значения вероятностей событий $H_1 - H_4$ существенно отличаются от их байесовских оценок, которые позволяют рассчитать обновленные значения вероятностей p_a, p_b, равные соответственно 0,601 и 0, 727. При поступлении новой информации полученные условные

вероятности событий $H_1 - H_4$ следует рассматривать как априорные, которые могут быть обновлены (уточнены) путем уже рассмотренного выше пересчета по формуле Байеса. В общем случае количество как возможных способов реализации атак, так и конкретных гипотез, составляющих полную группу событий, может быть более двух.

Выводы

Для современных ИКС, основой производственной и организационно-управленческой деятельности которых является бизнес-процесс, характерны непостоянство структуры и состава модели угроз, конечное время существования угрозы, изменение вероятности реализации угрозы в пределах времени ее существования и, как следствие, появление динамических рисков угроз. Кроме того, зависимость вероятности реализации угрозы от времени обусловила необходимость введения понятия терминальной вероятности и методов ее вычисления. Последние в статье представлены сценарным методом определения значений терминальной вероятности и экспертным, в котором реализована возможность обновления ранее полученных экспертных оценок за счет дополнительно поступающих новых сведений.

ЛИТЕРАТУРА

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. № 2657-XII.
2. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБ України від 08 листопада 2005 р. № 125.
3. Соснин А.С. Менеджмент безопасности предпринимательства: Учеб. пособие / А.С.Соснин, П.Я.Прыгунов. – К.: Изд-во Европ. ун-та, 2002. – 357 с.
4. Твердохліб М.Г. Інформаційне забезпечення менеджменту / М.Г. Твердохліб. – К.: КНЕУ, 2002. – 224 с.
5. Мильнер Б.З. Теория организаций / Б.З. Мильнер. – М.: ИНФРА-М, 1999. – 336 с.
6. Смирнов Э.А. Теория организации / Смирнов Э.А. – М.: ИНФРА-М, 2000. – 248 с.
7. Информационные технологии управления: Учебное пособие / Под. ред. Ю.М.Черкасова. – М.: ИНФРА-М, 2001. – 216 с.
8. Основы экономической информатики: Учеб. пособие / А.Н.Морозевич, Н.Н.Говядинова, Б.А.Железко и др.; Под общ. ред. А.Н.Морозевича. – Мн.: «Мисанта», 1998. – 438 с.
9. Системы управления гибким автоматизированным производством: Учеб. пособие / Под общ.ред. А.А.Краснопрошиной. – К.: Вища шк., 1987. – 383 с.
10. Ивашко В.Г. Экспертные системы и некоторые проблемы их интеллектуализации / В.Г.Ивашко, В.К.Финн // Семиотика и информатика, М.: ВИНИТИ, 1986. - №27. – С.25-61.
11. Информационные технологии организации бизнеса / [Карпенко С.В., Иванченко Е.В., Корченко А.А., Казмирчук С.В.]. – К.: Изд-во Национального авиационного ун-та, 2012. – 306 с.
12. Казмиренко В.П. Социальная психология организаций: Монография / В.П.Казмиренко. – К.: МЗУУП, 1993. – 384 с.
13. Смирнов Б.А. Методы инженерной психологии / Б.А.Смирнов, А.М.Тиньков. –Х.: Изд-во «Гуманитарный Центр», 2008. – 528 с.
14. Постанова Кабінету Міністрів України "Про затвердження Національної рамки кваліфікації" від 23 грудня 2011 р. №1341. [Электронный ресурс] – Режим доступа: http://zakon2.rada.gov.ua/laws/show/1341-2011-n/print133071182.
15. Архипов А.Е. Об особенностях оценивания вероятностей, используемых для вычисления информационных рисков.// Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту: Матеріали міжнародної наукової конференції (ISDMCI '2010). Том 2. – Херсон: ХНТУ, 2010. – 590с, с. 515-517.
16. Архипов А.Е. Применение среднего риска для оценивания эффективности защиты информационных систем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип.1 (14). – К.: 2007. – С.60-67.
17. Архипов А.Е. Экспертно-аналитическое оценивание информационных рисков и уровня эффективности системы защиты информации // Радіоелектроніка, інформатика, управління - 2009 - №1. - С. 58-61.
18. Архипов А.Е., Архипова С.А. Применение мотивационно-стоимостных моделей для описания вероятностных соотношений в системе «анализ-защита» / А.Е. Архипов, С.А.Архипова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип.1 (16). – К.: 2008. – С. 57-61.
19. Архипов А.Е. Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков / А.Е. Архипов // Захист інформації – № 2 (51), 2011. – С.69-76.

Надійшла: 7.11.2012 р.

Рецензент: д.т.н., професор Корченко О.Г.