ИНФОРМАТИКА

2005 **январь-март** **№1**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 681.324.067

В.В. Анищенко, А.М. Криштофик

О НЕОБХОДИМОСТИ РАЗРАБОТКИ МОДЕЛЕЙ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Проводится анализ наиболее известных моделей оценки защищенности объектов информационных технологий, рассматриваются их достоинства и недостатки. Обосновывается необходимость разработки новой модели объекта информационных технологий и средств защиты. Предлагается подход к построению модели на основе анализа рисков от реализации угроз безопасности.

Введение

Информационные системы относятся к критическим системам, поскольку при дальнейшей компьютеризации и интеллектуализации таких систем неизбежен парадокс, заключающийся в том, что фундаментальный источник технологического прогресса одновременно является и растущим источником технологической уязвимости. Зависимость критических систем от программно-технических средств порождает необходимость придания этим средствам заданных свойств качества, безопасности, способности противостоять разрушению, нарушениям функционирования системы, сбоям, преднамеренным воздействиям и ошибкам различных видов при выполнении критической системой основных целевых функций.

Большие объемы информации различной степени конфиденциальности, возможности доступа к отдельным элементам таких систем привели к возникновению множества угроз информационной безопасности. Это, в свою очередь, привело к разработке соответствующего этим угрозам множества специальных мер, средств и систем защиты информации (СЗИ) и, как следствие, разработке программно-технических средств, представляющих собой сложную организационно-техническую систему, характеризующуюся множеством разнородных параметров.

Под защитой информации принято понимать создание в объектах информационных технологий организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации [1].

Необходимость оценки эффективности обеспечения безопасности в объектах информационных технологий (ОИТ) обусловлена тем, что в наиболее общей формулировке целью создания СЗИ является достижение научно обоснованного уровня защищенности информации путем применения организованной совокупности методов и средств защиты. Исследование вопросов оценки эффективности обеспечения безопасности информации в ОИТ является основой разработки количественных требований к создаваемым СЗИ и их подсистемам. Оценка уровня безопасности разрабатываемых, выпускаемых и планируемых к разработке объектов (продуктов или систем) информационных технологий является одной из важнейших частей их создания. Такая оценка должна производиться на всех этапах жизненного цикла ОИТ при различной степени полноты и достоверности имеющейся информации. Основой для оценки защищенности ОИТ является его формальная модель, на основании которой производится оценка.

1. Нормативно-методическая база по вопросам оценки защищенности объектов информационных технологий

Основой для проведения любых работ в области информационной безопасности, в том числе и оценки защищенности, являются международные стандарты ISO 15408 и ISO 17799.

ISO 15408 Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий) определяет функциональные требова-

ния к механизмам безопасности программно-технического уровня и требования к адекватности их реализации. При оценке защищенности этот стандарт целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности с точки зрения полноты реализованных функциональных требований и надежности их реализации. Общие критерии определяют общую методологию оценки с учетом угроз, уязвимостей, активов, рисков нанесения ущерба и выбора контрмер (управления рисками). Они могут быть применены к механизмам безопасности организационного уровня и требований по физической защите, которые прямо связаны с функциональными требованиями.

ISO 17799 Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) наиболее полно определяет критерии для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты, а также десять практических рекомендаций по управлению информационной безопасностью и спецификации для проведения сертификации режима информационной безопасности. Данный стандарт предусматривает вопросы анализа и управления рисками и является наиболее распространенным в мире среди организаций и предприятий, которые используют подобные стандарты.

Для оценки защищенности кроме международных широко используются и национальные стандарты, такие как NIST SP 800 30, Sys Trust, BSI\IT Baseline Protection Manual, SAC, COSO, SAS 55/78, Cobit, предусматривающие вопросы анализа и управления рисками, и некоторые другие, аналогичные им. Для эффективного анализа и управления информационными рисками разработаны и широко применяются качественные и количественные международные методики. К этим методикам относятся COBRA, RA Software Tool, CRAMM, Risk Watch, Buddy System, Method Ware.

Указанные стандарты и методики, реализующие вопросы анализа и управления рисками, с той или иной мерой полноты и качества предполагают анализ и оценку рисков (активов, угроз, уязвимостей) и управление ими с целью выбора контрмер для снижения ущерба.

2. Анализ моделей системы обеспечения безопасности. Достоинства и недостатки

Формальная модель оценки защищенности объектов информационных технологий, по сути, является основой для понимания взаимодействия элементов «внешняя среда – объект информационных технологий – последствия», а также формализованным инструментом для получения аналитических выражений показателей защищенности (уязвимости) ОИТ и выбора варианта средств защиты информации. Она поясняет взаимодействие всех составляющих процесса нанесения ущерба владельцам активов.

Для обеспечения полной защиты активов (объектов защиты) в ОИТ каждый путь осуществления угрозы должен быть перекрыт соответствующим средством обеспечения безопасности (условие полного перекрытия). Данное условие является первым фактором, определяющим защищенность ОИТ. Второй фактор – это стойкость существующих средств обеспечения безопасности к попыткам их обхода либо преодоления, третий – величина ущерба, наносимого владельцу активов в случае осуществления угроз безопасности. При выполнении первого условия и идеальной стойкости средств обеспечения безопасности ущерб, наносимый владельцам активов, равен нулю, т. е. реализуется абсолютная защищенность ОИТ. Величина ущерба, наносимого владельцам активов, определяется первыми двумя факторами.

Рассмотрим основные математические модели, представляющие интерес с точки зрения их адекватности объектам информационных технологий и возможностей их практического использования.

Базовая модель системы защиты определяется взаимодействием трех множеств:

$T = \{t_i\}, i = \overline{1,I}$ – угроз безопасности, воздействующих на ОИТ;

$M = \{m_k\}, k = \overline{1,K}$ – средств обеспечения безопасности;

$O = \{o_j\}, j = \overline{1,J}$ – защищаемых объектов (рис. 1) [2].

В «защищенной» системе все ребра модели представляются в виде $\langle t_i m_k \rangle$ и $\langle m_k o_j \rangle$. Любое ребро $\langle t_i o_j \rangle$ определяет незащищенный объект (ребра $\langle t_1 o_2 \rangle$ и $\langle t_1 o_4 \rangle$ на рис. 1). При этом одно и то же средство обеспечения безопасности может перекрывать более одной угрозы и (или) защищать более одного объекта. Отсутствие ребра $\langle t_i o_j \rangle$ не гарантирует полной безопасности за счет того, что в действительности средства обеспечения безопасности, выполняя функцию «брандмауэра», создают некоторую степень сопротивления попыткам проникновения угроз, характеризующую их стойкость к воздействию угроз.

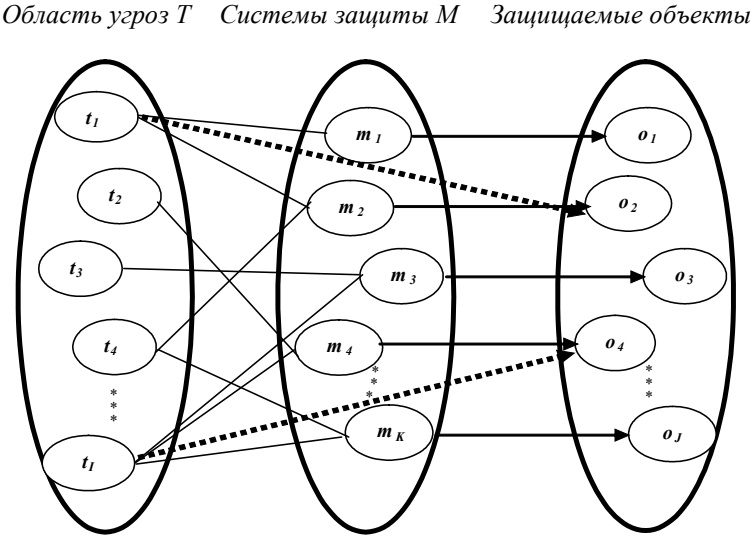

Рис. 1. Базовая модель системы защиты

В базовой модели системы защиты с полным перекрытием выполняется первое условие обеспечения полной защищенности ОИТ $\forall(t_i) \in T \quad \exists(m_k) \in M$, означающее, что для каждой угрозы t_i из множества угроз T существует средство обеспечения безопасности m_k из множества средств обеспечения безопасности M, перекрывающее путь проникновения этой угрозы к объекту защиты o_j. Эффективность защиты объектов в данной модели определяется вторым и третьим факторами, характеризующими защищенность ОИТ, т. е. стойкостью средств обеспечения безопасности и величиной ущерба, наносимого владельцам активов. Процесс анализа и оценки защищенности заключается в формировании перечня объектов защиты с определением их стоимости, полного перечня угроз и пространства их воздействий на объекты защиты, перечня СЗИ и пространства их воздействий на угрозы безопасности с оценкой их стойкости.

Данная модель явилась основой для разработки всех последующих моделей оценки защищенности ОИТ в различных ее модификациях.

Модель системы обеспечения безопасности Клементса представляет собой пятикортежный граф $S = \{O, T, M, V, B\}$ (рис. 2) [2]. В данной модели O – набор защищаемых объектов; T – набор угроз; M – набор средств обеспечения безопасности; $V = T \times O = \{v_r = \langle t_i, o_j \rangle, r = \overline{1, R}\}$ – набор уязвимых мест, представляющих собой пути проникновения угроз в систему; $B = V \times M = T \times O \times V = \{b_l = \langle t_i, o_j, m_k \rangle, l = \overline{1, L}\}$ – набор барьеров, представляющих собой точки, в которых требуется осуществлять защиту в системе. Для данной модели система защиты с полным перекрытием представляет собой систему, в которой имеются средства защиты на каждый возможный путь проникновения угроз. В такой системе для каждой уязвимости $v_r = \langle t_i, o_j \rangle \in V$ предусматривается наличие барьера $b_l = \langle t_i, o_j, m_k \rangle \in B$, создаваемого средством обеспечения безопасности m_k, в противном случае объект o_j не защищен при воздействии

некоторой угрозы t_i. Для оценки защищенности системы в данной модели использовались лингвистические переменные. Каждый элемент набора барьеров B представляет собой составную лингвистическую переменную b_l с тремя компонентами, составленными из имени и лингвистического значения (табл. 1).

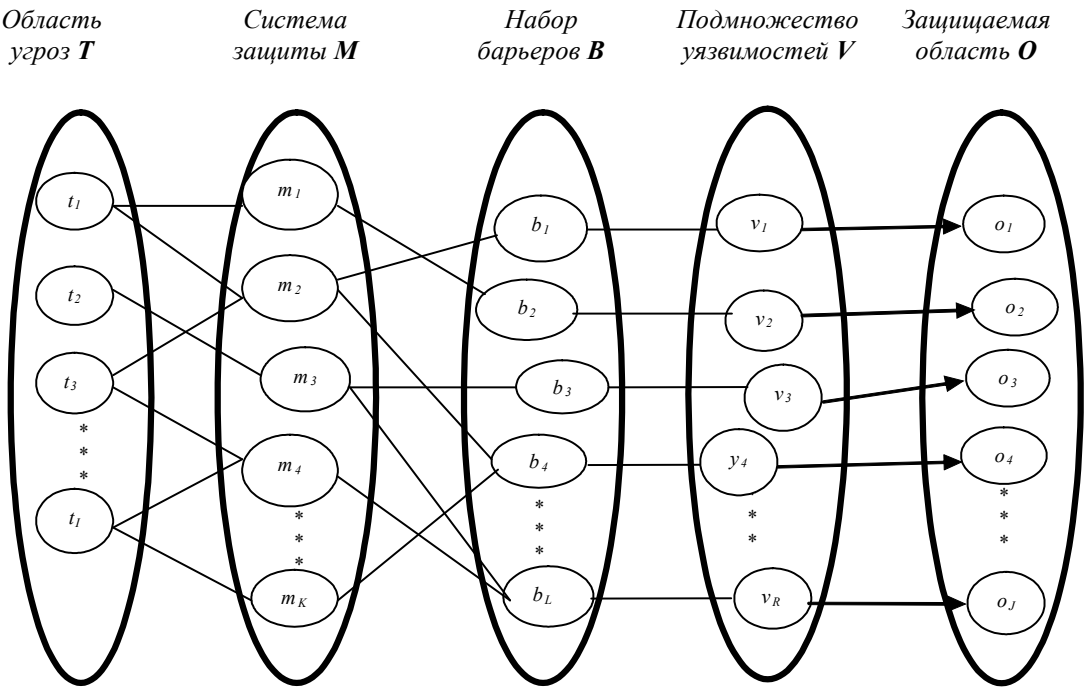

Рис. 2. Модель системы защиты, содержащей уязвимости

За счет использования большого количества лингвистических переменных автор модели получает большую степень уверенности в том, что конечная лингвистическая оценка правдоподобна.

Для данной модели условие полного перекрытия записывается в виде

$$\forall(v_r)\in V \;\; \exists\left(b_l = \langle t_i, m_k, o_j\rangle\right)\in B \;\; .$$

Это условие означает, что для каждой уязвимости v_r из множества уязвимостей V средством обеспечения безопасности m_k из множества средств обеспечения безопасности M создается барьер b_l из множества барьеров B, устраняющий эту уязвимость.

Таблица 1

Барьер защиты как составная лингвистическая переменная

Лингвистическая переменная	Имя	Лингвистическое значение
$\boldsymbol{b_l}$	$\boldsymbol{t_i}$	Вероятность проявления угрозы $\boldsymbol{P_l}$
	$\boldsymbol{o_j}$	Значение величины ущерба $\boldsymbol{L_l}$
	$\boldsymbol{m_k}$	Степень сопротивляемости средства защиты $\boldsymbol{R_l}$

В работе [3] для данной модели в качестве показателя прочности барьера $b_l = \langle t_i, o_j, m_k\rangle$ применяется остаточный риск, связанный с возможностью осуществления угрозы безопасности t_i в отношении объекта o_j при использовании механизма защиты m_k:

$$R_k = P_k L_k \left(1 - R_k\right),$$

где P_k – вероятность появления угрозы, против которой создан механизм защиты m_k;

L_k – величина ущерба защищаемых объектов при удачном осуществлении угрозы, против которой создан механизм защиты m_k,;

R_k – степень сопротивляемости механизма защиты m_k, характеризующаяся вероятностью его преодоления.

Показатель защищенности ОИТ определяется выражением

$$W = \frac{1}{\sum_{k=1}^{K} P_k L_k \left(1 - R_k\right)}.$$

Знаменатель этого выражения определяет суммарную величину остаточных рисков, связанных с возможностью осуществления угроз безопасности T в отношении объектов O при использовании механизмов защиты M. Суммарная величина остаточных рисков характеризует общую «уязвимость» системы защиты, а защищенность ОИТ определяется как величина, обратная уязвимости. Необходимо отметить, что для определения показателей прочности барьеров и защищенности ОИТ автор использует численные значения тех же компонент лингвистической переменной, что и в модели Клементса вместо лингвистических значений. Однако подходы к определению их численных значений автором не определены.

Достоинствами данной модели являются:

– формализация с использованием математического аппарата теории множеств;

– получение непрерывной интервальной оценки показателей защищенности и прочности барьеров;

– наглядное представление взаимодействия ее элементов.

Недостатки модели:

– является гипотетической, поскольку ее структура соответствует системе защиты с полным перекрытием, защищенность которой определяется только стойкостью средств обеспечения безопасности, что на практике никогда не выполняется; не учитывает среды безопасности, структуры построения объекта оценки (конфигурации) и вида обрабатываемой информации, т. е. не привязана к типу объекта оценки;

– не соответствует действующим нормативным документам в области защиты информации [4], поскольку не учитывает вопросов анализа рисков, не позволяет обоснованно проектировать профили защиты и задания по обеспечению безопасности, осуществлять выбор варианта средств защиты активов;

– не учитывает вопросы изменения уязвимостей ОИТ и рисков с введением в ее структуру средств обеспечения безопасности активов (остаточные уязвимости и остаточные риски);

– показатели защищенности не привязаны к разработанной модели, неправильно трактуется их физический смысл, поскольку риск нанесения ущерба определяет не стойкость средств обеспечения безопасности (хотя и зависит от нее), а возможность нанесения ущерба за счет слабости системы защиты, свойств ОИТ и характеристик угроз и, следовательно, не имеет размерности ущерба.

В работе [5] рассмотрена математическая модель комплексной оценки защищенности компьютерных систем (КС), которая построена на основе несколько измененной базовой модели системы защиты с полным перекрытием. В данной модели изменена последовательность сущностей системы в виде триады «СЗИ – угрозы – объекты защиты». Система безопасности представляется трехдольным графом (рис. 3), в котором вершины образуют три вектора-столбца:

$\overline{C}$ – весов СЗИ, определяемых соответствующей стоимостью;

$\overline{A}$ – весов угроз, описываемых вероятностями их проявления;

$\overline{R}$ – весов объектов защиты, определяемых величиной стоимости (ценности) объектов защиты.

В рамках теоретико-графового подхода дуги графа представляются в виде матриц смежности $E = \left(\overline{A}, \overline{R}\right) = \left\| e_{mn} \right\|$, $Z = \left(\overline{C}, \overline{A}\right) = \left\| z_{mk} \right\|$, элементы которых автором определены как вероятность возможности воздействия *m*-й угрозы на *n*-й объект защиты и вероятность нейтрализации *k*-м защитным средством *m*-й угрозы соответственно.

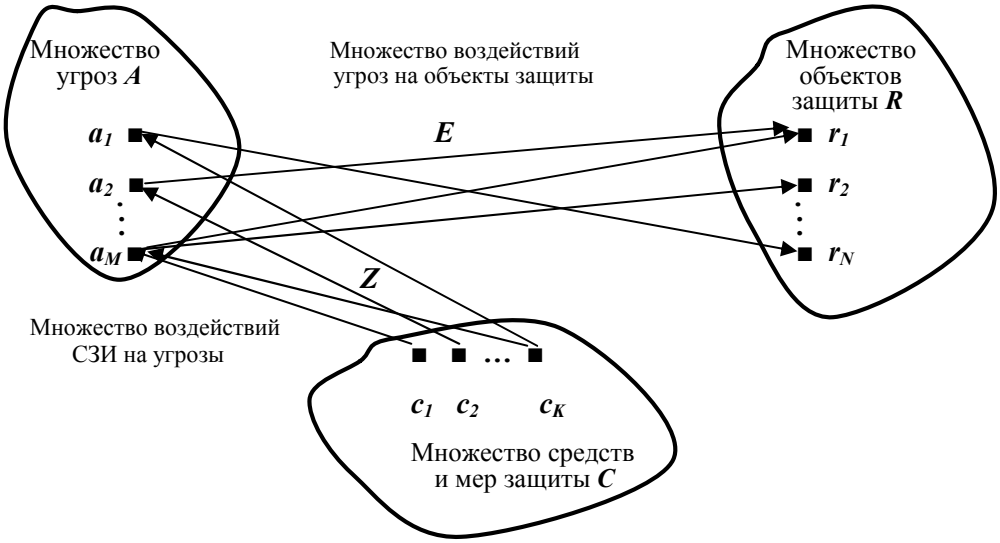

Рис. 3. Модель комплексной оценки защищенности КС

В качестве целевой функции при комплексной оценке защищенности используется величина потенциального ущерба от воздействия угроз безопасности

$$Э = \frac{C_0 - U}{C_0 + C_{СЗИ}},$$

где $C_0 = \sum_{n=1}^{N} r_n$ – стоимость объектов компьютерных систем;

$C_{СЗИ}$ – стоимость средств защиты информации;

$U = \sum_{n=1}^{N} r_n \left(1 - \prod_{m=1}^{M} e_{mn} \left(1 - a_m^* \right) \right)$ – ущерб от нарушения информационной безопасности при наличии СЗИ;

$a_m^* = a_m \left(1 - \prod_{k=1}^{K} \left(1 - z_{mk} \right) \right)$ – вероятность проявления *m*-й угрозы с учетом воздействия СЗИ.

Процесс анализа и оценки защищенности, как и в аналогичной модели [1], заключается в формировании перечня объектов защиты (моделировании КС) с оценкой их стоимости (первый этап); полного перечня угроз, а также пространства их воздействий на объекты защиты для конкретной КС с оценкой вероятностей проявления угроз (второй этап); перечня СЗИ и пространства их воздействий на угрозы безопасности с оценкой вероятности нейтрализации угроз (третий этап).

Разработка рассматриваемой модели проводилась в предположении, что при оценке защищенности КС с использованием риска результаты получаются в ранговой шкале «высокий –

приемлемый – незначительный» и не учитываются затраты, связанные с использованием СЗИ в отношении снижения потенциального ущерба от угроз безопасности.

Достоинством данной модели является получение показателя эффективности системы защиты в интервальной шкале от нуля до единицы.

Недостатки модели:

– является гипотетической, поскольку граничные значения показателя эффективности системы защиты не существуют (ноль соответствует условию, когда воздействие угроз приводит к ущербу, равному стоимости всей КС, а единица, когда система защиты полностью нейтрализует воздействие угроз при нулевых затратах на СЗИ); значение показателя эффективности является безразмерной величиной и характеризует относительный ущерб;

– не учитывает структуру построения (конфигурации), свойства (уязвимости) объекта оценки и вида обрабатываемой информации, т. е. не привязана к типу объекта оценки;

– не соответствует действующим нормативным документам в области защиты информации, поскольку не учитывает вопросы анализа рисков, риск не определяется стоимостными оценками;

– не позволяет обоснованно проектировать профили защиты и задания по обеспечению безопасности, осуществлять выбор варианта защиты активов на основе анализа рисков, как того требуют Общие критерии;

– показатели защищенности не имеют физического смысла, значение показателя эффективности характеризует не ущерб, а относительный ущерб, поскольку является безразмерной величиной.

В работе [6] произведена модификация рассмотренной модели с целью устранения ряда ее недостатков. Для модификации модели в целях привязки ее к типу объекта оценки и устранения ряда недостатков были введены два множества:

– видов информации $E = \{e_n\}, n = \overline{1, N}$, находящейся в объекте информационных технологий (ОИТ) и подлежащей защите;

– классов ОИТ $D = \{d_s\}, s = \overline{1, S}$, характеризующих структуру и конфигурацию их построения.

Множества видов информации $E = \{e_n\}, n = \overline{1, N},$ и классов ОИТ $D = \{d_s\}, s = \overline{1, S},$ образуют подмножество типов объектов оценки [7]

$$Q = D \times E = \{q_z = \langle d_s, e_n \rangle\}, z = \overline{1, Z}, \; Z < S \times N,$$

удовлетворяющее условию $(\exists d_s)(\exists e_n) \Rightarrow (\exists q_z)(q_z = \langle d_s, e_n \rangle)$, поскольку ОИТ определенных конфигураций не может работать со всеми видами информации ввиду невозможности обеспечения требуемой эффективности ее защиты.

Множество *T* угроз информационной безопасности, множество *O* объектов защищаемой системы и множество *M* средств обеспечения безопасности зависят от класса ОИТ и вида информации, находящейся в ОИТ, т. е. от типа объекта оценки. Вследствие этого существует набор правил $d_s, e_n \to t^*, d_s, e_n \to o^*, d_s, e_n \to m^*$, ставящих в соответствие каждому элементу (d_s, e_n) множества $\{D, E\}$ «класс ОИТ – вид информации» некоторые элементы t_i, o_j, m_k множеств *T, O, M*, образующих подмножества T^*, O^*, M^*, т. е. существуют функциональные отношения

$$T^* \subset Q \times T, \quad O^* \subset Q \times O, \quad M^* \subset Q \times M.$$

Это означает, что каждому элементу q_z множества типов объектов оценки *Q* соответствуют вполне определенные подмножества T_z^*, O_z^*, M_z^* [6, 7]. Введение подмножества типов

объектов оценки Q позволяет определить подмножества T^*, O^*, M^* как совокупность образов, получаемых при отображении подмножества Q на множества T, O и M соответственно:

$$Y^* : T \to Y, \;\; O^* : T \to O, \;\; M^* : T \to M.$$

Подмножества T_z^*, O_z^*, M_z^* удовлетворяют условиям

$$T = \bigcup_{z=1}^{Z} T_z^*, \; O = \bigcup_{z=1}^{Z} O_z^*, \; M = \bigcup_{z=1}^{Z} M_z^* .$$

В связи с практическим отсутствием систем защиты информации с полным перекрытием вводятся *системы защиты с частичным перекрытием*, для которых выполняется условие

$$\exists \left(v_r = \langle y_{i*}, o_{j*} \rangle \in V \right) \Rightarrow \; \bar{\exists} \left(m_k \right) \quad \left(b_l = < y_{i*}, o_{j*}, m_{k*} > \in B \right).$$

Это условие означает, что существуют угрозы, воздействующие на активы через определенные уязвимости, против которых не существует средств обеспечения безопасности m_{k*}, создающих устраняющие эти уязвимости барьеры. Однако такая модификация не устраняет всех недостатков модифицируемой модели, а только привязывает ее к типу объекта оценки и вводит системы защиты с частичным перекрытием, оставляя при этом основные ее недостатки.

В работе [8] предложена математическая модель защиты информации, которая наиболее полно характеризует взаимодействие составляющих процесса нанесения ущерба владельцам активов. Данная модель включает семь абстрактных пространств:

– источников угроз K;

– информационных объектов (объектов защиты) L;

– оценок важности информационных объектов V;

– средств противодействия (средств защиты) C;

– эффективности средств защиты информации H;

– оценок стоимости средств защиты Ψ;

– решений на основе возможных воздействий дестабилизирующих факторов на объект защиты и применения имеющихся средств защиты A.

Решающая функция, представляющая алгоритм реализации и координации действий средств защиты от угроз для объектов защиты, вместе с пространствами A, K, L, V, C, H образует математическую модель процесса защиты информации. Получение решающих функций в общем виде производится иерархично с последующим разбиением на уровни взаимодействия:

определенная угроза – способ ее реализации – объект защиты – средство защиты – оценка эффективности;

определенная угроза – способ ее реализации – объект защиты – все средства защиты – оценка эффективности;

определенная угроза – все способы ее реализации – объект защиты – все средства защиты – оценка эффективности;

все предполагаемые угрозы – все способы их реализации – объект защиты – все средства защиты – оценка эффективности;

все предполагаемые угрозы – все способы их реализации – все объекты защиты – все средства защиты – оценка эффективности.

Решающая функция в виде функционалов в явном виде будет определяться конкретными условиями обстановки (конкретным объектом защиты, источником угроз и способами их реализации, средствами противодействия и способами их применения для защиты информации). Предполагается, что функционалы будут носить вероятностный характер.

Достоинством данной модели является учет большого количества характеристик, влияющих на эффективность обеспечения безопасности. Недостатки модели:

– является абстрактной, поскольку не определяет критерии оценки эффективности средств обеспечения безопасности, что предполагает использование критериев по усмотрению разработчиков, не учитывает структуры построения объекта оценки (конфигурации) и вида обрабатываемой информации, т. е. не привязана к типу объекта оценки;

– не соответствует действующим нормативным документам в области защиты информации, поскольку не учитывает вопросов анализа рисков, не позволяет обоснованно проектировать профили защиты и задания по обеспечению безопасности;

– не учитывает вопросы процесса изменения структуры ОИТ с введением в ее структуру средств обеспечения безопасности активов (перехода уязвимостей и рисков в остаточные уязвимости и остаточные риски);

– не предусматривает возможности описания характеристик, влияющих на эффективность обеспечения безопасности, в различных шкалах измерений.

Проведенный анализ разработанных моделей оценки защищенности ОИТ показал, что они и, как следствие, показатели эффективности защиты не учитывают вопросов анализа рисков нанесения ущерба и управления ими. Это свидетельствует о их несоответствии требованиям действующих нормативно-технических документов в данной области.

С использованием указанных моделей разработано множество показателей защищенности ОИТ. Условно их можно разделить на стоимостные, функциональные и основанные на риске нанесения ущерба, однако показатели защищенности, основанные на риске, не связаны с моделью и ее составляющими, а разработаны отвлеченно от них.

Таким образом, разработанные к настоящему времени формальные модели оценки защищенности ОИТ обладают рядом общих недостатков. Это не позволяет использовать их для научно обоснованной разработки требований безопасности при проектировании профиля защиты (задания по безопасности), варианта средств обеспечения безопасности, выбора показателей эффективности защиты от угроз безопасности и, как следствие, оценки защищенности ОИТ.

3. Необходимость разработки базовой модели объекта информационных технологий

Проведенный анализ разработанных моделей показывает, что основным их недостатком является несоответствие действующим нормативным документам по вопросам обеспечения безопасности информационных технологий. Все разработанные модели не учитывают вопросов анализа рисков и разработки (выбора) на их основе средств обеспечения безопасности (управления рисками). В данных моделях сразу предполагается наличие средств обеспечения безопасности.

Для устранения недостатков рассмотренных моделей и, как следствие, привязки их к действующей нормативно-технической базе необходимо разработать новую формальную модель с учетом требований Общих критериев, других нормативных методических документов и программного обеспечения на основе оценки и анализа рисков.

Это предполагает разработку модели на основе анализа возможных негативных последствий от реализации угроз безопасности с учетом взаимодействия цепочки *«угроза – уязвимость – объект защиты – риск нанесения ущерба – контрмеры (средства защиты) – остаточная уязвимость – остаточный риск нанесения ущерба – допустимость остаточного риска»* [9]. Первые четыре элемента указанной цепочки определяют базовую модель ОИТ. Такая постановка вопроса позволяет не только оценивать эффективность средств обеспечения безопасности, но и задавать требования безопасности при проектировании профиля защиты (задания по безопасности), осуществлять правильный выбор варианта средств защиты, оценивать ущерб, наносимый владельцам активов. Она соответствует действующим и общепринятым мировым сообществом стандартам в области обеспечения безопасности информационных технологий.

Заключение

Анализ достоинств и недостатков основных моделей оценки защищенности ОИТ показал, что они не учитывают вопросов анализа рисков. Это приводит к несоответствию таких моделей принятым критериям оценки безопасности информационных технологий, что свидетельствует об их разработке до принятия Общих критериев. В связи с этим возникла необходимость в раз-

работке новой базовой модели ОИТ с учетом требований действующей нормативно-технической базы. Данная модель должна быть разработана на основе анализа негативных последствий от воздействия угроз безопасности с использованием методов оценки и анализа рисков. Выбор средств защиты активов должен осуществляться на основе принятой стратегии управления рисками с учетом существующих ограничений.

Список литературы

1. Петров В.А. Информационная безопасность. Защита информации от несанкционированного доступа в АС. – М.: МИФИ, 1993. – 78 с.

2. Хоффман Л.Дж. Современные методы защиты информации. – М.: Сов. радио, 1980. – 264 с.

3. Астахов А. Анализ защищенности корпоративных автоматизированных систем // http://www.cobit.ru/security/Pubs/Pub1_AAM_SecEval.htm.

4. СТБ 34.101.1 (ИСО/МЭК 15408-1). Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель.

5. Воронцов Ю.В., Гайдамакин Н.А. Модель комплексной оценки защищенности компьютерных систем в идеологии ущерба от угроз безопасности // Вопросы защиты информации. – № 1. – М., 2003. – С. 45–53.

6. Анищенко В.В., Криштофик А.М. Модификация графовой модели системы защиты информации // Тез. докл. VI военно-науч. конф. Военной академии Республики Беларусь. 25-26 ноября 2003 г. – Мн.: ВА РБ, 2003. – С. 89–90.

7. Анищенко В.В., Криштофик А.М. Классификация суперкомпьютерных систем кластерного уровня с позиций выполнения требований безопасности // Суперкомпьютерные системы и их применение: Докл. Междунар. науч. конф. SSA' 2004. 26-28 октября 2004 г., Минск. – Мн.: ОИПИ НАН Беларуси, 2004. – С. 233–237.

8. Костин Н.А. Актуальные вопросы теории защиты информации // Мат. Междунар. конф. «Безопасность информации». 14–18 апреля 1997 г., Москва. – М., 1997. – С. 98–109.

9. Анищенко В.В., Криштофик А.М. Методика оценки защищенности объектов информационных технологий при повышенных требованиях безопасности // Военно-техническая политика государства в современных условиях: Тез. докл. военно-науч. конф. 12–13 октября 2004 г., Минск. – Мн.: НИИ ВС РБ. – С. 198–200.

Поступила 06.04.04

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: anat@newman.bas-net.by

V.V. Anishchanka, A.M. Krishtophic

ON NECESSITY TO DEVELOP A MODEL OF INFORMATION TECHNOLOGY OBJECTS SECURITY

Based on analysis of existent models of protection evaluations, the necessity is shown to develop a new basic model of information technology objects. It involves the analysis of negative consequences of security threats, based on research of the elements interaction: «threat – vulnerability – asset – risk». Such an approach toward the development of a basic model meets the requirements of information technology security criteria. The model developed will enable to perform scientifically substantiated elaboration (selection) of security requirements and corresponding to the requirements measures.