ИНФОРМАТИКА

2008 **январь-март** **№ 1**

УДК 004.05

А.М. Криштофик

МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА С УЧЕТОМ РИСКОВ ОСТАТОЧНЫХ УЯЗВИМОСТЕЙ

Предлагается модель системы защиты активов на основе методологического подхода, базирующегося на системном анализе рисков и требованиях действующей нормативной базы. В основу разработки положена базовая модель объекта информационных технологий (ОИТ). Вводятся и определяются термины остаточных уязвимостей, рисков и ущербов; производится классификация систем защиты.

Введение

Необходимость в создании новой модели системы защиты ОИТ обусловлена тем, что разработанная базовая модель [1] и ее модификации обладают рядом недостатков, ограничивающих их использование [2]. Наиболее существенным недостатком является несоответствие модели и ее модификаций методологии, принятой в критериях оценки безопасности информационных технологий (ИТ), которые являются основополагающим действующим международным стандартом в этой области [3], и нормативным документам, применяемым для базового уровня и повышенных требований безопасности [4]. Это ограничивает их использование при разработке требований безопасности в процессе проектирования профиля защиты (задания по безопасности) и показателей защищенности, выборе варианта средств защиты и, как следствие, при проведении оценки защищенности. Структура модели не учитывает анализ рисков при разработке (выборе варианта) средств защиты информации (СЗИ), которые сразу вводятся в ее состав. Такая модель не позволяет предъявлять требования к СЗИ, оптимизировать процесс выбора варианта средств защиты. Показатели защищенности не связаны со структурой этой модели, что привело к большому разнообразию подходов к их разработке [5].

1. Характеристика средств защиты информации

Оценка рисков является необходимым и достаточным условием для решения задачи управления рисками, которая включает выбор и обоснование выбора контрмер, позволяющих снизить величины рисков до приемлемых значений. Управление рисками также включает в себя оценку стоимости реализации контрмер, которая должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть тем больше, чем меньше риск нанесения ущерба. Уменьшение рисков может осуществляться комплексно с применением различных способов (таблица) [6]. Цель защиты активов от несанкционированных действий (НСД) с использованием аппаратно-программных СЗИ состоит в том, чтобы по возможности перекрыть пути воздействия угроз на активы (ребра в графе «угроза – уязвимость» модели ОИТ [7]). Она достигается путем введения требуемого множества СЗИ $M = \{m_q\}$.

По принципам действия средства защиты можно разделить на две группы (рис. 1):

– создающие определенные барьеры защиты и снижающие уязвимость ОИТ (идентификация, аутентификация, управление доступом и др.);

– обнаруживающие вторжения и создающие барьеры защиты.

СЗИ первой группы выполняют функции защиты по отношению к определенным уязвимостям объекта оценки (ОО), которые связаны с определенными угрозами, коррелированными с этими уязвимостями, и опосредованно – по отношению к активам; СЗИ второй группы – по отношению к угрозам и уязвимостям, коррелированным с этими угрозами, и опосредованно – к активам.

СЗИ создают определенные барьеры, перекрывающие пути проникновения угроз через уязвимости к активам и характеризующие их стойкость по предотвращению воздействия угрозы определенного вида через определенную уязвимость.

Таблица

Способы управления рисками информационной безопасности

Элемент безопасности	Управление рисками информационной безопасности		Область использования
	Способ защиты	Мера защиты	
Угрозы безопасности	Уменьшение вероятностей осуществления	Организационно-правовые (законодательные, административные, процедурные и физические меры защиты)	Политика безопасности, задачи безопасности
	Выявление (обнаружение и предотвращение) атак и других нарушений информационной безопасности	Аппаратно-программные средства	Разработка и эксплуатация СЗИ
Уязвимости ОИТ	Снижение (устранение) уязвимостей	Организационные (административные, процедурные и физические меры защиты)	Политика безопасности
		Аппаратно-программные средства	Разработка и эксплуатация СЗИ
Активы ОИТ	Защита активов	Аппаратно-программные (криптографические) средства	Разработка и эксплуатация СЗИ
		Организационные (административные, процедурные и физические меры защиты)	Политика безопасности, задачи безопасности
	Восстановление	Резервное копирование	Политика безопасности
Ущерб	Передача	Страхование	Политика безопасности
	Принятие	Отсутствуют	Политика безопасности

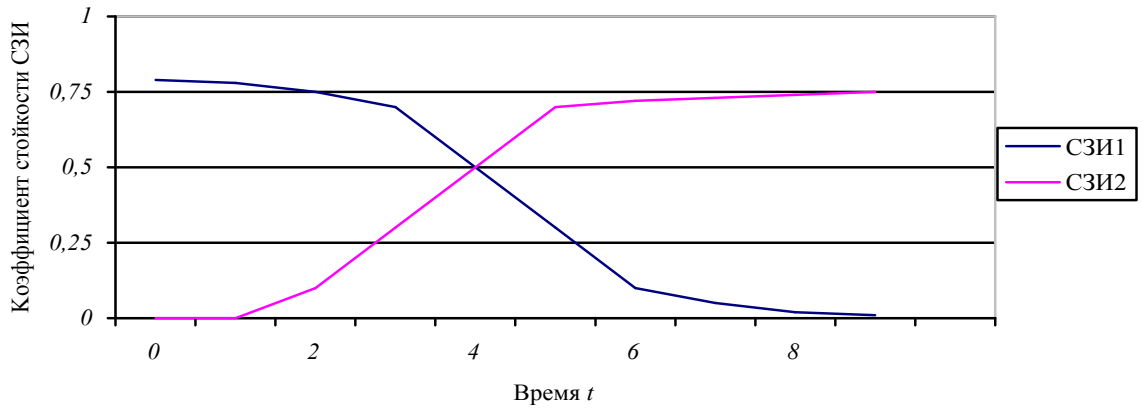

Рис. 1. Зависимость коэффициента стойкости от времени для двух типов СЗИ

Барьер – способность СЗИ перекрывать вероятный путь реализации определенной угрозы через соответствующую уязвимость на некоторую область активов, характеризующая их стойкость, т. е. это способность СЗИ снижать уязвимости ОИТ от воздействия угрозы.

Множество барьеров B, создаваемых СЗИ, определяется декартовым произведением множеств угроз, СЗИ и уязвимостей, через которые воздействуют угрозы $B = Y \times M \times V = \{b_l = \langle y_i, m_q, v_k \rangle\}$, $l \equiv iqk = \overline{1,L}$, $L = I \times Q \times K$. Не каждый член декартова произведения $B = Y \times M \times V$ образует барьер к данному виду угроз $(\exists y_i)(\exists m_q)(\exists v_k) \Rightarrow$

$\Rightarrow (\exists b_l)\ \left(b_l = \langle y_i, m_q, v_k \rangle = 0\right)$, так как СЗИ выполняет свои функции только по отношению к определенным видам угроз, воздействующим на активы через уязвимости. Каждое СЗИ m_q создает подмножество барьеров b_l для снижения определенных уязвимостей при реализации угроз, т. е. выполняется условие $(\forall m_q \in M)\ (\exists v_k \in V)(\exists y_i \in Y)\ (b_l = \langle y_i m_q v_k \rangle)$.

Каждому элементу множества барьеров $B = \{b_l\} = (\langle y_i, m_q, v_k \rangle)$ приписан вес α_l, являющийся элементом нечеткого множества $W = \{\alpha_l,\ \mu_l\}$, характеризующий стойкость данного СЗИ по перекрытию пути ($i \to k$) проникновения угрозы y_i через уязвимость v_k; $\mu_l = \mu_{q_{ik}}$ – совместная функция принадлежности элемента $\alpha_l = \alpha_{q_{ik}}$ нечеткому множеству $W = \{\alpha_{q_{ik}}, \mu_{q_{ik}}\}$. Стойкость СЗИ $\alpha_l = \alpha_{q_{ik}} = 1/k_{q_{ik}}$, где $k_{q_{ik}} \in (1, \infty]$ – коэффициент снижения уязвимости, $k_{q_{ik}} = 1$ при отсутствии СЗИ m_q на пути реализации угрозы ($i \to k$). В качестве характеристики СЗИ можно также использовать коэффициент $\beta_l = \beta_{q_{ik}} = (1 - \alpha_{q_{ik}})$, характеризующий величину сниженной (предотвращенной) уязвимости.

Коэффициент стойкости принимает значения:

$$\alpha_{q_{ik}} := \begin{cases} \alpha_l \in [0,1) & \text{ï ðè} \quad m_q = 1, \\ 1 & \text{ï ðè} \quad m_q = 0 \end{cases}$$

или

$$\beta_{q_{ik}} = \begin{cases} \beta_l \in (0,1] & \text{ï ðè} \quad m_q = 1, \\ 0 & \text{ï ðè} \quad m_q = 0. \end{cases}$$

Условие $\beta_1 = 1$ при $m_q = 1$ выполняется при наличии СЗИ с идеальной стойкостью, т. е. полностью перекрывающего путь проникновения угрозы (на практике не существует). В этом случае справедливо соотношение $\alpha_l = 1 - \beta_l = 0$ при $m_q = 1$. Если описание характеристик α_l, β_l проводится в шкалах измерений, выходящих за пределы интервала [0,1], то они нормируются по отношению к максимально возможной величине.

СЗИ, выполняя свои функции, определенным образом создают барьеры на пути реализации:

– нескольких разных угроз через определенную уязвимость

$$(\exists m_q \in M)(\exists v_k \in V)(\exists y_i \in Y) \quad \exists \left(\{b_l\} = \{\langle y_i, m_q, v_k \rangle, i = \{i^*\}, i^* = \overline{1, I^*}, I^* \in I, q \in Q, k \in K\} \right);$$

– одной угрозы через несколько определенных уязвимостей

$$(\exists m_q \in M)(\exists v_k \in V)(\exists y_i \in Y) \quad \exists \left(\{b_l\} = \{\langle y_i, m_q, v_k \rangle, i \in I, q \in Q, k = \{k^*\}, k^* = \overline{1, K^*}, K^* \in K\} \right);$$

– нескольких определенных угроз через несколько определенных уязвимостей

$$(\exists m_q \in M)(\exists v_k \in V)(\exists y_i \in Y) \quad \exists \left(\{b_l\} = \{\langle y_i, m_q, v_k \rangle, i \in I, q = \{q^*\}, q^* = \overline{1, Q^*}, Q^* \in Q, k \in K\} \right);$$

– одной угрозы через одну определенную уязвимость

$$(\exists m_q \in M)(\exists v_k \in V)(\exists y_i \in Y) \quad \exists \left(\{b_l\} = \{\langle y_i, m_q, v_k \rangle, i \in I, q = \{q^*\}, q^* = \overline{1, Q^*}, Q^* \in Q, k \in K\} \right).$$

При наличии нескольких средств защиты $m_{q^*}, q^* = \overline{1, Q^*}, Q^* \in Q$, выполняющих свои функции по перекрытию пути реализации определенной угрозы y_i через определенную уязвимость v_k,

суммарный коэффициент стойкости определяется выражениями $\alpha_{l_\Sigma} = \alpha_{q_{\Sigma}\, ik} = \prod_{q^*=1}^{Q^*} \alpha_{q^*\, ik}$ и $\beta_{l_\Sigma} = \beta_{q_{\Sigma ik}} = \left(1 - \prod_{q^*=1}^{Q^*} \alpha_{q^*\, ik}\right)$.

Анализ рисков нанесения ущерба позволяет сформулировать количественные требования к стойкости СЗИ. Требуемая стойкость СЗИ определяется как отношение допустимого остаточного риска к риску нанесения ущерба $\alpha_{l\,\text{треб}} = r_{ikj\ \text{доп}} \big/ \overline{r_{ikj}}$, характеризующее необходимую степень снижения риска нанесения ущерба владельцам активов СЗИ от воздействия определенной угрозы через соответствующую уязвимость на определенную область активов, где $\overline{r_{ikj}}$ – оценочное значение риска.

Данная характеристика барьера введена в рассмотренном выше виде, в отличие от модели системы защиты Клеменса [1], чтобы показать, что барьер – это характеристика СЗИ, а не элемент безопасности, влияющий на процесс нанесения ущерба в результате нарушения информационной безопасности. Элементами безопасности являются сами средства защиты, которые не полностью перекрывают определенные уязвимости по отношению к действию определенных угроз и определенных уязвимостей, поскольку одна и та же уязвимость может быть использована различными видами угроз для нарушения безопасности.

2. Классификация систем защиты

В зависимости от условий выбора требуемых СЗИ ($r_c > 0$ или $\mathrm{r}_c > \mathrm{r}_{c\,\text{доп}}$) и от степени защищенности активов можно выделить системы защиты с полным перекрытием и системы защиты с частичным перекрытием [2, 12, 13].

Система защиты активов с полным перекрытием – это система, в которой для каждой угрозы и уязвимости ОО существуют СЗИ $\left(\forall y_i \in Y\right)\left(\forall v_k \in V\right)\left(\mathrm{r_c} = (y_i\, v_k\, a_j) \neq 0\right)$ $\left(\exists m_q \in M\right)\left(b_l = \langle y_i, m_q, v_k\rangle \in B\right)$, создающие барьеры, которые снижают или устраняют эти уязвимости. В данной модели стойкость СЗИ определяет остаточный риск $R^{\otimes} = \left\{r^{\otimes}_{c_\gamma} = \langle y_i, v_k, m_q, a_j\rangle\right\}, c_\gamma = \overline{1, C}$. Недостатками модели являются отсутствие учета стоимости СЗИ и, как следствие, экономическая нецелесообразность ее использования. При обеспечении полной защищенности активов получается идеальная модель защиты активов.

Идеальная система защиты – это гипотетическая система защиты с полным перекрытием, обеспечивающая отсутствие остаточных уязвимостей, т. е. $\left(\forall y_i \in Y\right)\left(\forall v_k \in V\right)\times$ $\times\left(\mathrm{r_c} = (y_i\, v_k\, a_j) \neq 0\right)\left(\exists m_q \in M\right)\left(\left(v_{k^*} = (v_k\ m_q) = 0\right)\right)$. Для таких систем требуются СЗИ, полностью перекрывающие пути проникновения угроз и устраняющие уязвимости ОИТ.

На практике СЗИ обеспечивают лишь некоторую (частичную) степень сопротивляемости угрозам безопасности с определенной степенью доверия. Это обусловлено тем, что разработка СЗИ безопасности проводится в условиях частичной априорной неопределенности относительно угроз безопасности и уязвимостей ОО, а также тем, что СЗИ, являясь составной частью ОИТ, сами подвержены воздействию угроз и имеют собственные уязвимости. Поэтому для существующих систем защиты суммарная уязвимость системы отлична от нуля.

Если необходимый набор СЗИ определяется при условии допустимости риска, то проектируется система защиты с частичным перекрытием.

Система защиты с частичным перекрытием – это система защиты, в которой существуют угрозы и уязвимости (не перекрытые СЗИ), создающие риски нанесения ущерба, меньшие допустимого значения. Для таких систем выполняется условие частичного перекрытия

$$(\exists y_i \in Y)(\exists v_k \in V)\left(r_c = \langle y_i, v_k, a_j \rangle\right) \Rightarrow \left(\overline{\exists} m_q\right)\left(b_l = \langle y_i, m_q, v_k \rangle \in B\right).$$

Степень перекрытия СЗИ путей реализации угроз является первым фактором, определяющим защищенность ОИТ, вторым фактором является их стойкость. Оба эти фактора будут учтены при разработке модели. Они в полной мере характеризуют систему защиты ОИТ и определяют эффективность защиты активов.

3. Остаточные уязвимости

Введение в ОИТ множества СЗИ, создающих определенные барьеры, приводит к изменению его структуры и характеристик множества уязвимостей, т. е. появлению остаточных уязвимостей.

Остаточная уязвимость – это уязвимость ОИТ, которая характеризует свойства и состояние ОИТ и СЗИ, способствует осуществлению угрозы или которая может быть использована для осуществления угрозы и неперекрытая СЗИ, а также уязвимость, неперекрытая СЗИ и обусловленная конечной их стойкостью (рис. 2).

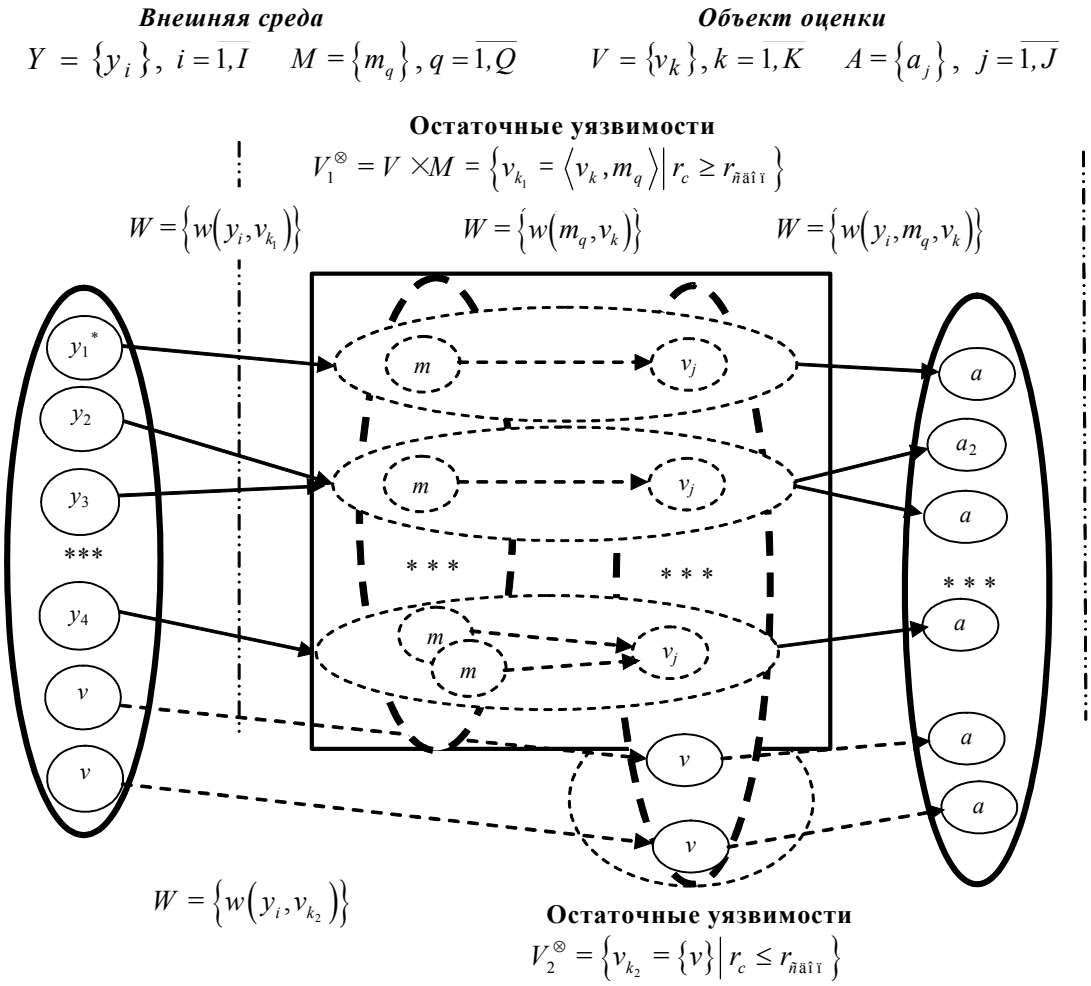

Рис. 2. Модель остаточной уязвимости ОИТ

Множество остаточных уязвимостей определим как объединение двух подмножеств $V^{\otimes} = \left\{v_{k^{\otimes}}\right\} = V_1^{\otimes} \cup V_2^{\otimes}$ (рис. 2), где $V_1^{\otimes} = V \times M = \left\{ v_{k_1} = \langle v_k, m_q \rangle \middle| r_c = \left(y_i\, v_k\, a_j\right) > r_{\text{ñäîï}} \right\}$, $k_1 = \overline{1, K_1}$, $K_1 = K \times Q$, – подмножество уязвимостей, перекрытых СЗИ и обусловленных их ограниченной стойкостью, которое определяется декартовым произведением множеств уязви-

мостей V и СЗИ M ОО; $V_2^{\otimes} = \left\{ v_{k_2} \,\middle|\, r_c = \left(y_i \; v_k \; a_j \right) \le r_{c\text{äîï}} \right\}, V_2^{\otimes} \subset V, k_2 = \overline{1, K_2}, K_2 \subset K$, – подмножество уязвимостей, не перекрытых СЗИ; $k^{\otimes} = \overline{1, \sum_{\xi=1}^{2} K_\xi}$ – общее количество остаточных уязвимостей.

Некоторые СЗИ могут полностью перекрыть пути проникновения угроз, что приводит к устранению существовавших уязвимостей, т. е. некоторые комбинации «уязвимость – средство защиты» декартова произведения $\langle v_{k*}, m_q \rangle$ образуют нулевую остаточную уязвимость $\exists \left(m_q \right) \; \exists \left(v_{k*} = \langle v_k, m_q \rangle = 0 \right)$. Данное условие выполняется за счет создания СЗИ, полностью перекрывающего путь проникновения угрозы. Некоторые элементы множества $V^{\otimes}$ могут быть равны соответствующим элементам уязвимостей V. Это означает, что для данных уязвимостей, т. е. для случая $r_c \le r_{c\,\text{доп}}$, не созданы СЗИ.

Введение в модель СЗИ приводит к изменению характеристик двудольного H-вершинного графа $G = (Y, V, E_H)$, $Y = \{y_i\}$, $V = \{v_k\}$, $i = \overline{1, I}$, $k = \overline{1, K}$, и базовой модели ОИТ [7], характеризующего взаимодействие множеств угроз безопасности и уязвимостей ОО. Изменяются характеристики ребер $E_H = \{e_h\} = \{e_{ij}\}$, $h = \overline{1, H}$, $H < I \times J$, т. е. характеристики нечеткого множества $W = \{w_{ik}, \mu_{ik}\}$ за счет изменения характеристик $K_k = (k_k, \mu_k(k))$ множества уязвимостей $V = \{v_k\}$, $i = \overline{1, I}$, $k = \overline{1, K}$ (рис. 3).

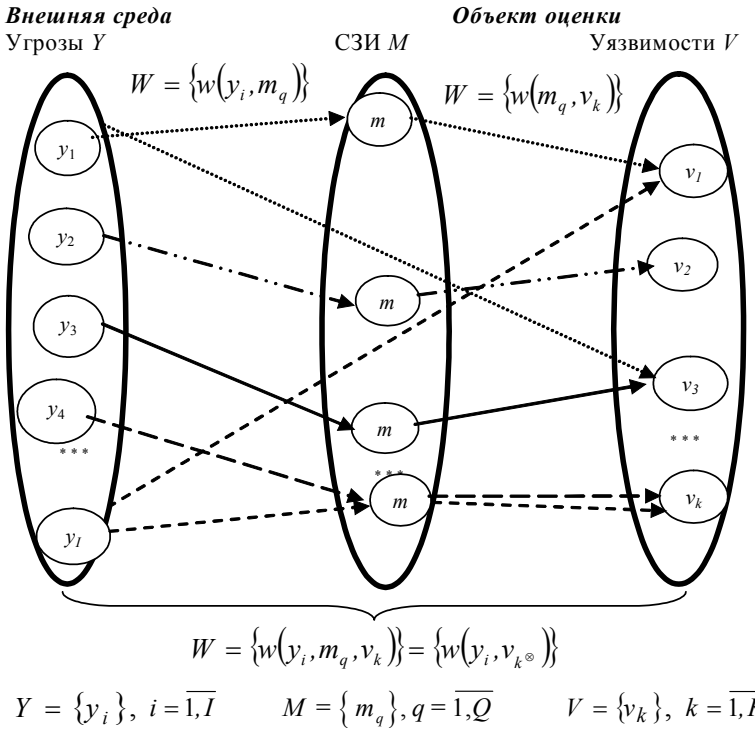

Рис. 3. Модель взаимодействия «угроза – средство защиты – уязвимость»

В данном случае характеристики ребер $E_H = \{e_h\} = \{e_{ij}\}$, $h = \overline{1, H}$, $H < I \times J$, описываемых нечетким множеством $W = \{w_{ik}, \mu_{ik}\}$, заменяются характеристиками двух двудольных графов:

$$G = (Y, M, E_H),\; Y = \{y_i\}, M = \{m_q\},\; i = \overline{1, I}, q = \overline{1, Q}\;;$$

$$G = (M, V, E_H),\; M = \{m_q\}, V = \{v_k\},\; q = \overline{1, Q}, k = \overline{1, K}\;.$$

Результирующее множество ребер $E_H = \{e_h\} = \{e_{iqj}\}, h = \overline{1,H}, H < I \times Q \times J$, описывается нечетким множеством $W = \{w_{iqk}, \mu_{iqk}\}$ и характеризует результаты этого взаимодействия.

4. Модель системы защиты информации

С позиций системного подхода, учета соотношения стоимости СЗИ, возможного ущерба от реализации угроз и при условии, что он превышает некоторую допустимую величину, множество СЗИ определим как

$$M_{\text{òðåá}} = \begin{cases} M = A = Y \times V = \{m_q\} = \{\langle y_i, v_k \rangle\}; \\ m_{q_{ik}} = \begin{cases} 1 \quad \text{ï ðè} \quad \left[\left(u_{ikj} > u_{\text{cäîï}} \right) \wedge \left(u_{ikj} > s_{mq} \right) \wedge \left(t_{ikj} < t_{qi} \right) \right], \\ 0 \quad \text{ï ðè} \quad \left[\left(u_{ikj} \le u_{\text{cäîï}} \right) \vee \left(u_{ikj} \le s_{m_q} \right) \vee \left(t_{ikj} \ge t_{qi} \right) \right]; \end{cases} \\ \mathrm{S}_m = \sum_q \mathrm{s}_{m_q} \le \mathrm{S}_{\text{äîï}}; \\ q \equiv ik, q = \overline{1,Q}, \ Q \le I \times K, \end{cases}$$

где y, v, u – элементы множеств угроз Y, уязвимостей V и ущербов U соответственно; $u_{c\,\text{доп}}$ – порог незначительности (допустимости) ущерба; S_m, s_{m_q} – стоимости всех СЗИ и конкретного средства m_q соответственно; $S_{\text{äîï}}$ – ограничения на стоимость СЗИ; 1, 0 – значения истинности и ложности высказывания «наличие элемента множества СЗИ», характеризующие наличие и отсутствие элемента m_q соответственно; t_{ikj}, t_{qi} – время реализации угрозы по пути $\left(y_i \to v_k \to a_j\right)$ и время реакции СЗИ m_q по перекрытию пути воздействия угрозы соответственно [8]. Для средств защиты второй группы необходимо дополнительно выполнить условие $t_{ikj} > t_{qi}$ (соотношение времени реализации угрозы t_{ikj} и времени реакции СЗИ t_{qi}). Важно, что при его невыполнении использовать данное СЗИ нецелесообразно.

Исходя из допустимого остаточного ущерба, который может быть различным для разных активов в зависимости от их важности и характера, можно определить значения элементов множества допустимых рисков $R_{\text{äîï}} = \{r_{c\,\text{äîï}}\}$, $r_{ikj\,\text{доп}} = u_{ikj\,\text{доп}} / s_j$. Тогда множество СЗИ можно определить через допустимый риск:

$$M_{\text{òðåá}} = \begin{cases} M = A = Y \times V = \{m_q\} = \{\langle y_i, v_k \rangle\}; \\ m_{qj} = m_{ikj} = \begin{cases} 1 \quad \text{ï ðè} \quad \left[\left(r_{ikj} > r_{c\,\text{äîï}} \right) \wedge \left(u_{ikj} > s_{mq} \right) \wedge \left(t_{ikj} > t_{qi} \right) \right]; \\ 0 \quad \text{ï ðè} \quad \left[\left(r_{ikj} \le r_{c\,\text{äîï}} \right) \vee \left(u_{ikj} \le s_{mq} \right) \vee \left(t_{ikj} \le t_{qi} \right) \right]; \end{cases} \\ S_m = \sum_{\text{q}} s_{m_q} \le S_{\text{äîï}}; \\ q \equiv ik, q = \overline{1,Q}, \ Q \le I \times K. \end{cases}$$

Снижение уязвимостей ОИТ за счет создания барьеров СЗИ приводит к снижению рисков, т. е. появлению остаточных рисков.

Остаточный риск – это мера, характеризующая потенциальную возможность непреднамеренного или умышленного нанесения ущерба владельцам активов посредством реализации угроз безопасности через уязвимости, не перекрытые средствами защиты, а также в обход или через них.

Множество остаточных рисков так же, как и множество остаточных уязвимостей, состоит из двух подмножеств

$$R^{\otimes} = \left\{ r_{c_\gamma}^{\otimes} \right\} = R_1^{\otimes} \cup R_2^{\otimes} = \left\{ r_{c_1}^{\otimes} = \langle y_i, v_{k_1}, a_j \rangle \right\} \cup \left\{ r_{c_2}^{\otimes} = \langle y_i, v_{k_2}, a_j \rangle \right\},$$

где $R_1^{\otimes} = \left\{ r_{c_1}^{\otimes} = \langle y_i, v_k, m_q, a_j \rangle \right\} \Big| \, r_{c_1} = \left(y_i \, v_k a_j \right) > r_{\text{сдоп}}$, $c_1 = \overline{1, C_1}$, – остаточный риск, обусловленный ограниченной стойкостью СЗИ;

$R_2^{\otimes} = \left\{ r_{c_2}^{\otimes} = \langle y_i, v_k, a_j \rangle \right\} \Big| \, r_c = \left(y_i \, v_k a_j \right) \le r_{\text{сдоп}}$, $c_2 = \overline{1, C_2}$, – остаточный риск, обусловленный уязвимостями, против которых не создано СЗИ;

$c_\gamma = \overline{1, (C_1 + C_2)}$ – количество элементов множества остаточных рисков.

Множество остаточных рисков характеризует меру возможного ущерба, наносимого владельцу активов при успешном осуществлении угрозы через определенные уязвимости, недостаточно перекрытые или не перекрытые СЗИ, на определенные области активов. Некоторые элементы множества остаточных рисков равны нулю. Это обусловлено тем, что есть активы, связанные с уязвимостями и угрозами, для которых существуют СЗИ, полностью перекрывающие пути проникновения угроз. Это приводит к отсутствию остаточных уязвимостей, т. е. некоторые комбинации $\left(y_i, v_{k*}, a_j \right)$ не создают остаточного риска $(\exists y_i)(v_{k*})(\exists a_j) \Rightarrow \left(\bar{\exists} r_{c*}\right) \ \left(r_{c*} = \langle y_i, v_{k1}, a_j \rangle \right)$. Оценки элементов множества остаточных рисков $r_{c1}^{\otimes} = y_i \cdot v_k \cdot m_q \cdot a_j$ и $r_{c2}^{\otimes} = y_i \cdot v_k \cdot a_j$ принимают значения $r_{c^*} \in [0; r_c]$.

Множество остаточных рисков определяет множество остаточных ущербов *U*, наносимых владельцам активов в результате реализации угроз безопасности через определенные уязвимости на определенные активы.

Остаточный ущерб – мера, характеризующая негативные последствия для владельцев активов от реализации угроз безопасности через определенные уязвимости на определенные области активов в обход/через СЗИ.

Множество остаточных ущербов определим как произведение множества остаточных рисков *R* и множества ценностей активов *S*, подлежащих защите: $U^{\otimes} = R^{\otimes} \times S = \left\{ u_c^{\otimes} \right\} = \left\{ r_c^{\otimes}, s_c^{\otimes} \right\}, c^* = \overline{1, C^*}$, где $s_{c^{\otimes}}$ – элемент множества S, характеризующий ценность *j*-го актива, для которого существует остаточный риск нанесения ущерба $r_{c*} = r_{ik*j}$.

Множество остаточных ущербов так же, как и множество остаточных рисков, состоит из двух подмножеств

$$U^{\otimes} = \left\{ u_{c_\gamma}^{\otimes} \right\} = U_1^{\otimes} \cup U_2^{\otimes} = \left\{ u_{c_1}^{\otimes} = \langle r_{c_1}^{\otimes}, s_{c_1}^{\otimes} \rangle \right\} \cup \left\{ u_{c_2}^{\otimes} = \langle r_{c_2}^{\otimes}, s_{c_2}^{\otimes} \rangle \right\},$$

где $U_1^{\otimes} = \left\{ u_{c_1}^{\otimes} = \left\langle < y_i, v_k, m_q, a_j >, s_j \right\rangle \right\} \Big| \, r_{c_l} = \left(y_i \, v_k a_j \right) > r_{\text{сдоп}}$, $c_1 = \overline{1, C_1}$, – остаточный ущерб, обусловленный ограниченной стойкостью СЗИ;

$U_2^{\otimes} = \left\{ u_{c_2}^{\otimes} = \left\langle < y_i, v_k, a_j >, s_j \right\rangle \right\} \Big| \, r_c = \left(y_i \, v_k a_j \right) \le r_{\text{сдоп}}, c_2 = \overline{1, C_2}$, – остаточный ущерб, обусловленный уязвимостями, против которых не создано СЗИ;

$c_\gamma = \overline{1, (C_1 + C_2)}$ – количество элементов множества остаточных рисков.

В результате получаем систему, состоящую из шести элементов $< Y, M, V, A, R^{\otimes}, U^{\otimes} >$, описывающую взаимодействие элементов безопасности, которые характеризуют внешнюю среду безопасности, ОО с учетом СЗИ и последствия от нарушения безопасности (рис. 4), и удовлетворяющую условиям

$$(\exists y_i)(\exists v_k) \ \left(r_c = (y_i \, v_k \, a_j) \le r_{c\,\text{доп}} \right) \Rightarrow \left(\bar{\exists} m_q \right) \ \left(m_q = \langle y_i, v_k \rangle \right);$$

$$(\exists y_i)(\exists v_k) \ \left(r_c = (y_i, v_k, a_j) > r_{c\,\text{доп}} \right) \Rightarrow \left(\exists m_q \right) \ \left(m_q = \langle y_i, v_k \rangle \right).$$

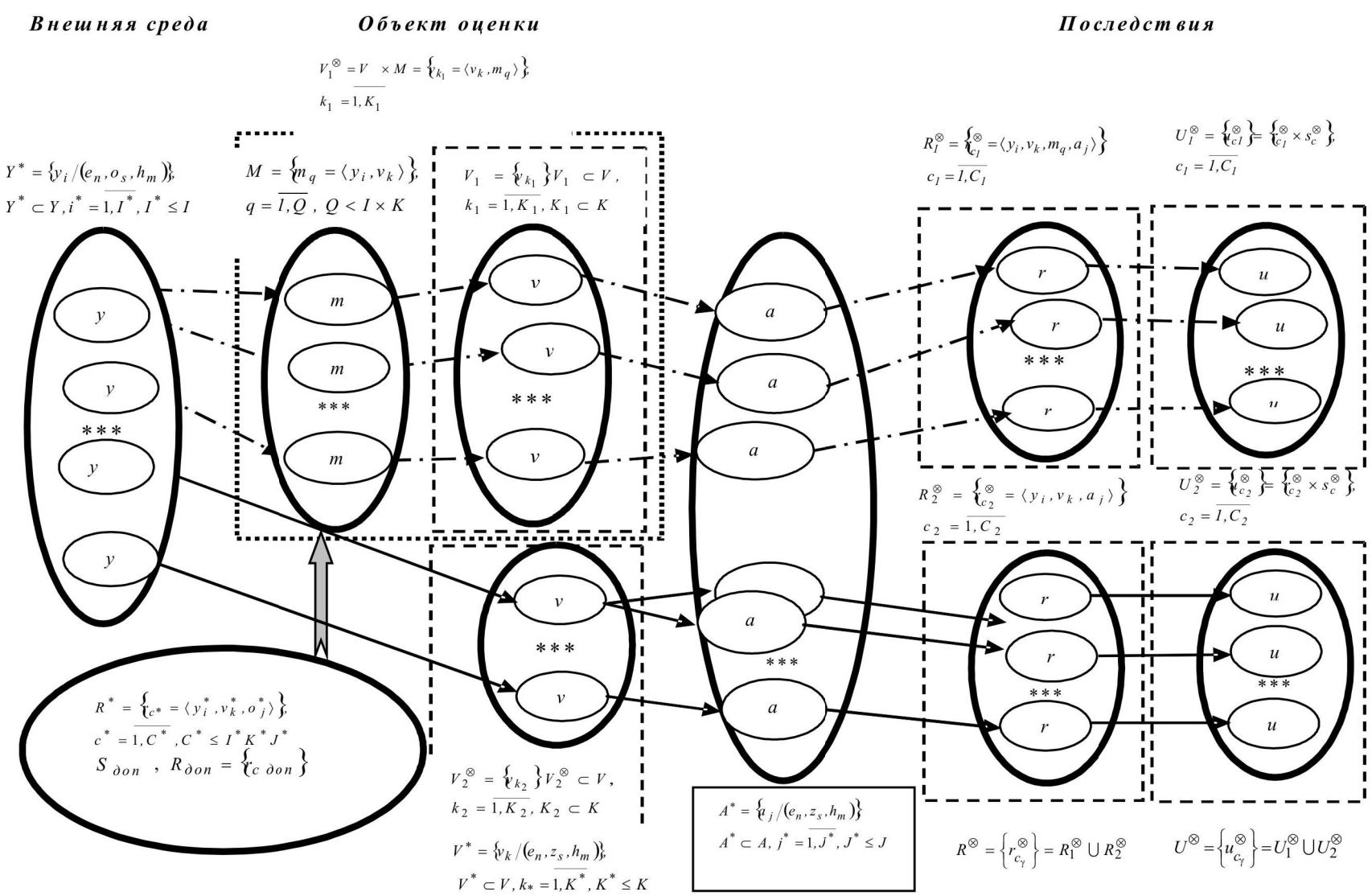

Рис. 4. Модель системы защиты

Формальная модель системы защиты поясняет взаимодействие всех составляющих процесса нанесения ущерба владельцам активов с учетом используемых СЗИ. Она является формализованным инструментом для получения аналитических выражений показателей защищенности, определения необходимого состава и требований к стойкости СЗИ для выполнения ТБ на основе анализа существующих и остаточных рисков от реализации угроз безопасности.

Разработанная модель:

– отражает процесс нанесения ущерба в результате нарушения безопасности с учетом наличия СЗИ;

– описывает изменение структуры ОИТ и его свойств с введением в его состав СЗИ, а также изменение последствий нарушения безопасности;

– учитывает стойкость СЗИ и позволяет предъявлять требования к ним.

Подход к построению модели напрямую можно использовать для разработки функциональных требований безопасности при проектировании профиля защиты (задания по безопасности) [9]. В этом случае элементы множества рисков должны быть классифицированы как риск нарушения определенной функции безопасности в соответствии с критериями оценки [10]. Классификация угроз безопасности в этом случае производится также в зависимости от характера риска нарушения функций безопасности. Такая классификация угроз рассмотрена в работе [11]. Таким образом, разработанная базовая модель системы защиты, в отличие от существующих, поясняет процессы создания эффективной системы защиты, нанесения ущерба при наличии СЗИ, формирования остаточных уязвимостей, влияния различных факторов на этот процесс. Она позволяет оценить величину остаточного риска и может использоваться как для разработки СЗИ, так и для оценки защищенности с учетом наличия СЗИ в составе ОИТ.

Заключение

Оценка уровня безопасности разрабатываемых, выпускаемых и планируемых к разработке ОИТ является одной из важнейших частей их создания и должна производиться на всех этапах жизненного цикла ОИТ при различной степени полноты и достоверности имеющейся информации. Решение этого вопроса предполагает конкретизацию задач и требований безопасности, описания ОО, показателей защищенности либо уязвимости ОО.

Разработанная формализованная модель системы защиты активов может быть использована для решения следующих частных задач при оценке безопасности ИТ:

– определения активов, требующих защиты;

– определения угроз безопасности активов;

– формулирования задач и требований безопасности;

– формирования (определения) функциональных и гарантийных требований типового ОО при проектировании профиля защиты (задания по безопасности);

– определения степени защищенности информационных ресурсов в ОО;

– выбора варианта СЗИ в разрабатываемом ОО;

– оценки рисков для выбранного варианта СЗИ;

– принятия решения о допустимости остаточного риска.

Список литературы

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

2. Анищенко, В.В. О необходимости разработки моделей защищенности объектов информационных технологий / В.В. Анищенко, А.М. Криштофик // Информатика. – № 1 (5). – 2005. – С. 122–131.

3. Криштофик, А.М. Нормативно-методическая база в области информационной безопасности. Состояние и перспективы развития / А.М. Криштофик // Информатика. – № 3 (11). – 2006. – С. 101–111.

4. Анищенко, В.В. Методы оценки эффективности защиты активов в объектах информационных технологий / В.В. Анищенко, А.М. Криштофик // Информатика. – № 3. – 2004. – С. 95–105.

5. Анищенко, В.В. Методология управления информационной безопасностью / В.В. Анищенко, А.М. Криштофик // Материалы XI Междунар. конф. «Комплексная защита информации». – Минск: Амалфея, 2007. – С. 23–28.

6. Анищенко, В.В. Базовая модель объекта информационных технологий / В.В. Анищенко, А.М. Криштофик // Информатика. – № 3 (7). – Минск: ОИПИ НАН Беларуси, 2005. – С. 116–125.

7. Криштофик, А.М. Управление информационной безопасностью на основе системного анализа рисков / А.М. Криштофик, В.В. Анищенко // Докл. Пятой Междунар. конф. «Обработка информации и управление в чрезвычайных и экстремальных ситуациях». – Т. 2. – Минск: ОИПИ НАН Беларуси, 2006. – С. 117–122.

8. Анищенко, В.В. Методика разработки функциональных требований безопасности на основе системного анализа рисков / В.В. Анищенко, А.М. Криштофик // Докл. БГУИР: материалы докл. и краткие сообщения III Белорусско-российской науч.-техн. конф. «Технические средства защиты информации», 23–27 мая 2005 г., Минск – Нарочь. – 2005. – № 5. – С. 7.

9. Information technology – Security techniques – Evaluation criteria for IT security. Part 1: Introduction and general model. – ISO/IEC 15408-1:2005; Part 2: Security functional requirements. – ISO/IEC 15408-2:2005; Part 3: Security assurance requirements. – ISO/IEC 15408-3:2005.

10. Сидак, А.А. Структура представления модели угроз безопасности при формировании профилей защиты информационных технологий / А.А. Сидак // Докл. Третьей Междунар. конф. «Цифровая обработка данных и ее применение» (DSPA-2000). – Т. 1. – СПб.: АВТЭКС, 2000. – С. 31–33.

11. Анищенко, В.В. Базовая модель системы защиты активов объекта информационных технологий / В.В. Анищенко, А.М. Криштофик // Докл. БГУИР: материалы докл. и краткие сообщения II Белорусско-российской науч.-техн. конф. «Технические средства защиты информации», 17–21 мая 2004 г., Минск – Нарочь. – 2004. – № 5. – С. 9.

12. Анищенко, В.В. Актуальные вопросы оценки защищенности информационных систем военного назначения / В.В. Анищенко, А.М. Криштофик // Наука и военная безопасность. – 2005. – № 1. – С. 30–34.

Поступила 10.05.07

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

A.M. Krishtophic

MODEL OF INFORMATION TECHNOLOGIES OBJECT PROTECTION SYSTEM

A model of an assets protection system on the basis of the methodological approach grounded on the system analysis of risks and common criteria requirements is developed. The base model for information technologies object is a basis of the development. The terms for residual vulnerabilities, risks and damages are introduced and defined. Classification of protection systems is made.