ИНФОРМАТИКА

2005 **июль-сентябрь** **№ 3**

УДК 681.324.067

В.В. Анищенко, А.М. Криштофик

БАЗОВАЯ МОДЕЛЬ ОБЪЕКТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

На основе методологии Общих критериев разработан общий подход к построению моделей объектов информационных технологий и систем защиты с использованием методов анализа рисков. Разработаны базовая модель объекта информационных технологий, обобщенные и частные интегральные показатели защищенности. Предложен метод адаптации базовой модели к типам объектов оценки. Определены основные направления использования базовой модели объекта информационных технологий.

Введение

Необходимость оценки защищенности объектов информационных технологий (ОИТ) обусловлена тем, что в наиболее общей формулировке целью создания средств обеспечения безопасности является достижение научно обоснованного и экономически целесообразного уровня защищенности путем применения организованной совокупности методов и средств защиты. Следовательно, исследование вопросов оценки защищенности ОИТ является основой для обоснования состава и количественных требований к создаваемым средствам безопасности и их подсистемам, проведения их доработок и модернизации. Оценка уровня защищенности планируемых к разработке, разрабатываемых, выпускаемых и находящихся в эксплуатации ОИТ является одной из важнейших частей их создания и эксплуатации. Такая оценка должна проводиться на всех этапах жизненного цикла ОИТ при различной степени полноты и достоверности имеющейся информации. Основой для оценки защищенности ОИТ является его формальная модель [1]. Однако разработанная базовая модель системы защиты и ее модификации обладают рядом недостатков, ограничивающих их использование [2]. Основными недостатками являются:

– несоответствие методологии, принятой в Общих критериях безопасности информационных технологий [3], т. е. они не учитывают вопросов анализа рисков при разработке (выборе варианта) средств обеспечения безопасности активов, которые сразу вводятся в состав модели;

– отсутствие взаимосвязи элементов безопасности, влияющих на защищенность ОИТ, и их изменение;

– невозможность разработки требований безопасности при проектировании профилей защиты (задания безопасности) объектов оценки;

– гипотетичность моделей (рассматриваются абстрактные системы защиты с полным перекрытием), отсутствие четкой взаимосвязи показателей защищенности со структурой модели;

– невозможность обоснования состава и характеристик выбранного варианта средств обеспечения безопасности.

В целях устранения указанных недостатков целесообразно разработать базовую модель объектов информационных технологий, на основании которой построить соответствующую модель системы защиты.

1. Разработка базовой модели объекта информационных технологий

1.1. Методологический подход к разработке базовой модели

Организация обеспечения безопасности активов должна носить комплексный характер и основываться на глубоком анализе возможных негативных последствий от реализации угроз безопасности. Это предполагает проведение оценки рисков информационной безопасности от реализации предполагаемых угроз с учетом наносимого при этом ущерба [4]. Основной методологический подход оценки защищенности ОИТ (рис. 1) определен Общими критериями [3].

Анализ негативных последствий предполагает обязательную идентификацию возможных нарушителей (источников угроз), факторов (уязвимостей), способствующих их проявлению; определение актуальных угроз безопасности информации, возможных негативных последствий реализации угроз (рисков нанесения ущерба); анализ возможного ущерба, наносимого владельцам активов. Результаты анализа являются исходными данными для выбора контрмер, способствующих минимизации возможного ущерба или снижению его до приемлемой величины. Такой подход позволяет обеспечить научно обоснованный и экономически целесообразный уровень защищенности ОИТ.

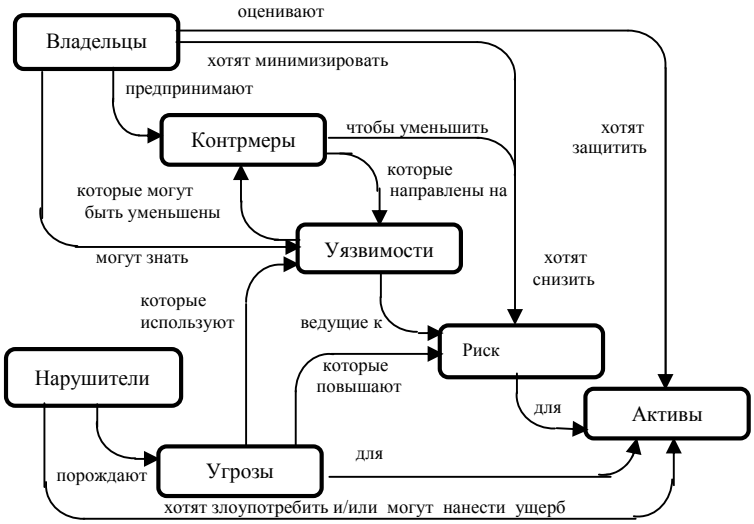

Рис. 1. Участники процесса нанесения ущерба и их взаимосвязь

Исходя из указанного принципа и требований нормативно-технических документов, решение задачи построения моделей ОИТ и системы защиты, оценки их защищенности предлагается проводить на основе анализа взаимодействия элементов безопасности в следующей последовательности: «*угроза* (действие) $\Rightarrow$ *уязвимость* (фактор) $\Rightarrow$ *актив* (объект) $\Rightarrow$ *риск* (возможность последствий) $\Rightarrow$ *ущерб* (последствия) $\Rightarrow$ *контрмеры* (противодействие) $\Rightarrow$ *остаточная уязвимость* (остаточный фактор) $\Rightarrow$ *остаточный риск* (остаточные возможности последствий) $\Rightarrow$ *остаточный ущерб* (остаточные последствия)».

Графическая модель взаимодействия рассматриваемых элементов безопасности отражает процесс возникновения риска нанесения ущерба, изменения структуры ОИТ и последствий от реализации угроз безопасности с введением средств обеспечения безопасности (остаточные уязвимости и риски). Она является основой для разработки базовой модели ОИТ с использованием взаимодействия элементов безопасности, характеризующих внешнюю среду и объект оценки без учета средств обеспечения безопасности и последствия этого взаимодействия (рис. 2).

1.2. Базовая модель объекта информационных технологий

В основу разработки базовой модели ОИТ без средств обеспечения безопасности положим взаимодействие элементов безопасности по схеме «внешняя среда безопасности – объект оценки – последствия» без использования средств обеспечения безопасности [2, 5–7]. Внешняя среда и ОИТ характеризуются взаимодействием следующих множеств:

– угроз активам $Y = \{y_i\}$, $i = \overline{1, I}$, исходящих из окружающей среды объекта, создающих опасность для его работы и требующих защиты активов;

– активов (информации или ресурсов) $O = \{o_j\}$, $j = \overline{1, J}$, характеризующих структуру и назначение ОИТ и подлежащих защите;

– уязвимостей $V = \{v_k\},\ k = \overline{1,K}$, характеризующих свойства ОИТ и его состояние и способствующих успешному осуществлению угрозы.

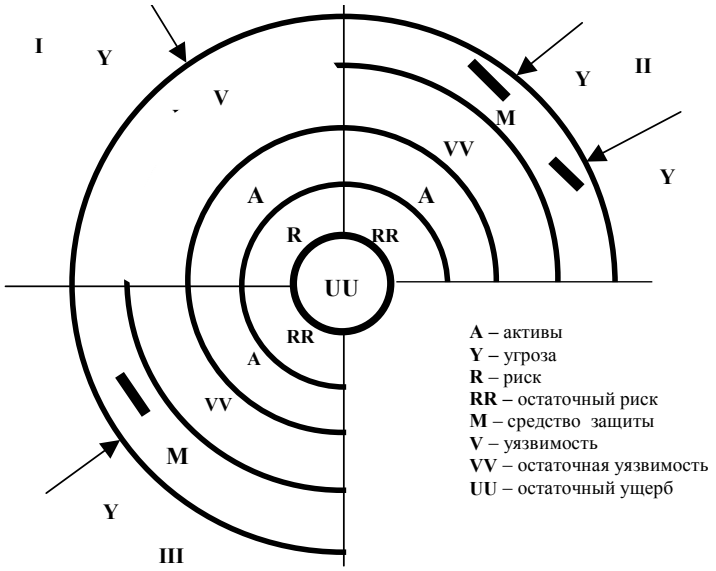

Рис. 2. Модель взаимодействия элементов безопасности

Существование однозначных взаимосвязей между некоторыми элементами множеств угроз безопасности *Y*, уязвимостей ОИТ *V* и активов *O* приводит к возможности нанесения ущерба владельцам активов. Следовательно, результатом взаимодействия этих множеств является множество рисков нанесения ущерба *R*, определяемое декартовым произведением множеств угроз, уязвимостей и активов $R = Y \times V \times O = A \times O = \left\{r_c = r_{ikj} = \langle y_i, v_k, o_j \rangle\right\}, c = \overline{1,C}, C = I \times K \times J$. Оно характеризует меру потенциальной возможности непреднамеренного или умышленного нанесения ущерба владельцу активов при успешном осуществлении определенной угрозы через соответствующую уязвимость на определенную область активов. Элемент множества рисков $r_c \equiv r_{ikj}$ характеризует возможность нанесения ущерба при реализации угрозы *i*-го вида через уязвимость *k*-го типа на *j*-ю область активов. Некоторые комбинации $\langle y_i, v_k, o_j \rangle$ не создают риска, поскольку существуют активы, связанные с уязвимостями, но для которых не существует угроз, или активы, для которых существуют угрозы, но эти угрозы не связаны с уязвимостями, т. е. выполняется условие $(\exists y_i)(\exists v_k)(\exists o_j) \Rightarrow (\overline{\exists} r)\ \left(r_c = \langle y_i, v_k, o_j \rangle\right), y_i \in Y, v_k \in V, o_j \in O, r_c \in R$. В этом случае элемент множества рисков принимается равным нулю.

Множество рисков определено в соответствии с введенным ранее определением [6, 8].

Риск нанесения ущерба – мера, характеризующая потенциальную возможность непреднамеренного или умышленного нанесения ущерба владельцам активов посредством реализации угроз безопасности через установленные уязвимости на определенные области активов.

В глоссарии терминов по информационной безопасности приводится восемь определений риска нарушения безопасности, в той или иной степени коррелированных между собой, при 16 определениях угрозы и 13 определениях уязвимости, взятых из зарубежных источников [9]. Отличительной особенностью введенного определения риска нанесения ущерба является привязка к конкретным активам. Это определение риска, в отличие от приведенных в работе [9], соответствует методологии Общих критериев и позволяет:

– непосредственно оценивать ущерб, наносимый владельцам активов вследствие нарушения безопасности, как основной показатель защищенности;

– учитывать ценность активов с позиций нарушителей информационной безопасности, характеризующую степень их заинтересованности в нарушении информационной безопасности;

– учитывать важность активов с позиции необходимости обеспечения различных уровней требований безопасности (например, базовый, средний, высокий) к разным активам;

– использовать как качественные, так и количественные методы оценки риска в любой шкале измерений, при любом априорно известном и доступном для исследователя числе характеристик угроз, уязвимостей и активов, а также объединять качественные и количественные показатели в интегральный показатель защищенности ИС.

Реализация определенной угрозы через определенную уязвимость на определенные активы приводит к нанесению ущерба владельцам активов, т. е. к возникновению множества ущербов.

Множество ущербов, наносимых владельцам активов вследствие реализации угроз безопасности, определяется произведением множества рисков нанесения ущерба и множества ценностей активов $U = R \times S = \{u_c = u_{ikj}\} = \{r_c, s_j\}$, $c = \overline{1,C}$, $j = \overline{1,J}$, где s_j – элемент множества ценностей активов j-го вида, для которых существует риск нанесения ущерба r_{ikj}.. Оно характеризует возможные потери, наносимые владельцам активов в результате нарушения их доступности, целостности и конфиденциальности.

Ущерб – мера, характеризующая негативные последствия для владельцев активов от реализации угроз безопасности через определенные уязвимости на определенные области активов.

Элементы этих множеств находятся между собой в определенных отношениях, описывающих ОИТ и характеризующих возможности воздействия угроз на определенные области активов через определенные уязвимости объекта оценки и последствия этого воздействия, т. е. риск нанесения ущерба владельцам активов и предполагаемый ущерб от нарушения безопасности. В результате получается пятиэлементный граф взаимодействия элементов безопасности *«угроза – уязвимость – актив – риск – ущерб»,* который представляет собой формальную базовую модель объекта оценки без средств обеспечения безопасности активов (рис. 3).

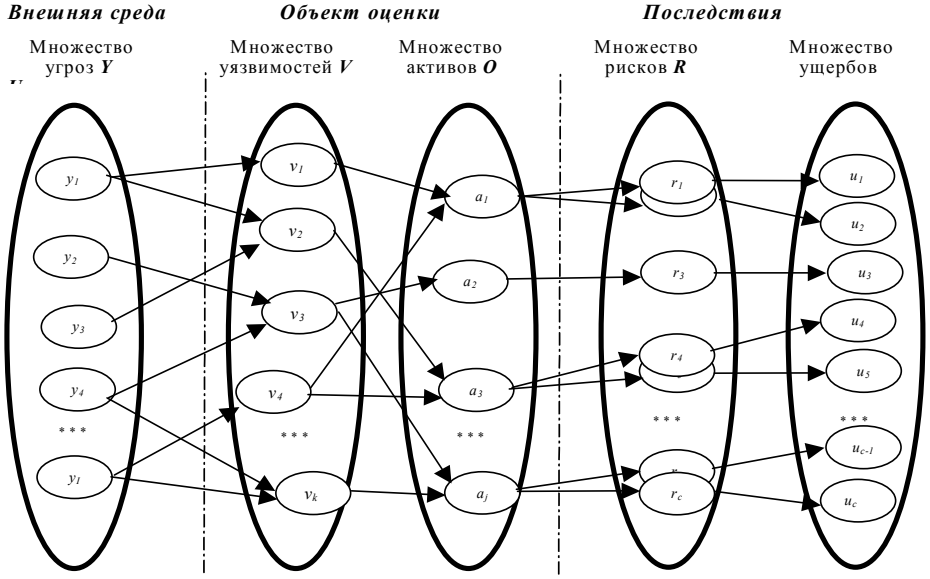

Рис. 3. Базовая модель объекта информационных технологий

Базовая модель ОИТ поясняет взаимодействие всех составляющих процесса нанесения ущерба владельцам активов и может быть использована как основа для проведения детального анализа рисков на этапе проектирования средств обеспечения безопасности. Она является формализованным инструментом для получения аналитических выражений показателей защищенности ОИТ с учетом всех характеристик модели, задания требований безопасности и определения требуемого состава средств обеспечения безопасности для выполнения требований безопасности на основе анализа рисков и соответствует первому типовому подходу оценки рисков информационной безопасности [4] при некоторой его модификации, заключающейся в переходе от рисков нарушения информационной безопасности к рискам нанесения ущерба и

ущербам непосредственно. Однако разработанная базовая модель ОИТ, как и существующие модели систем защиты [1, 2], является абстрактной. Для использования данной модели в практических приложениях необходимо конкретизировать множества элементов безопасности, характеризующих конкретный объект оценки и определяющих последствия нарушения информационной безопасности, т. е. необходимо провести адаптацию к типу объекта оценки [10, 11].

2. Адаптация базовой модели к типу объекта оценки

Существующие подходы адаптации моделей к объекту оценки основаны, как правило, на использовании двух дополнительных множеств: видов информации $E = \{e_n\}, n = \overline{1, N}$, находящейся в ОИТ и подлежащей защите, и классов ОИТ $Z = \{z_b\}, b = \overline{1, B}$, определяемых его составом и конфигурацией [10–12]. Однако указанные дополнительные два множества не в полной мере характеризуют объект оценки с точки зрения информационной безопасности. Уровни описания объекта оценки в соответствии с требованиями Общих критериев [3], а также способы формулирования требований и спецификаций для разработки профиля защиты и задания по обеспечению безопасности предполагают проведение анализа и оценки среды безопасности.

Среда безопасности включает:

– определение внешних условий, в которых предполагается использовать объект (свойств среды функционирования, политики безопасности организации);

– назначение ОИТ (тип объекта и сферу его применения);

– активы, которые требуют защиты и к которым относятся требования или политики безопасности;

– существующие или потенциальные угрозы в данной среде.

Результаты анализа среды безопасности являются исходной информацией для формулирования задач безопасности.

Следовательно, объект оценки (ОО) характеризуется своей *структурой* (назначением, составом, конфигурацией), *видом активов* (ценностью, важностью, возможностью восстановления), подлежащих защите, и *условиями эксплуатации*, характеризующими среду безопасности.

На основании вышеизложенного дополнительно введем множество классов ОИТ $Z = \{z_b\}, b = \overline{1, B}$, определяемых его составом и конфигурацией; множество видов информации $E = \{e_n\}, n = \overline{1, N}$, находящейся в ОИТ и подлежащей защите; множество условий эксплуатации $H = \{h_m\}, m = \overline{1, M}$. По аналогии с работами [4, 9] сформируем три условных подмножества:

Y^* – угроз безопасности, характерных для ОИТ определенной структуры, эксплуатируемого в определенной среде безопасности и содержащего различную по ценности и важности информацию;

O^* – подлежащих защите активов ОИТ определенной структуры, эксплуатируемого в определенной среде безопасности, содержащего различную по ценности и важности информацию;

V^* – уязвимостей ОИТ определенной структуры, эксплуатируемого в определенной среде безопасности и содержащего различную по ценности и важности информацию.

Данные подмножества определим как

$$Y^* = Y/(Z,E,H) = \{y_{i*}(z_b, e_n, h_m)\} = \{y_i/(z_b, e_n, h_m)\}, Y^* \subset Y, i^* = \overline{1, I^*}, I^* \le I;$$

$$O^* = O/(Z,E,H) = \{o_{j*}(z_b.e_n, h_m)\} = \{o_j/(z_b, e_n, h_m)\}, O^* \subset O, j^* = \overline{1, J^*}, J^* \le J;$$

$$V^* = V/(Z,E,H) = \{v_{k*}(z_b, e_n, h_m)\} = \{v_k/(z_b, e_n, h_m)\}, V^* \subset V, k^* = \overline{1, K^*}, K^* \le K.$$

Эти выражения означают, что существует набор правил $z_b, e_n, h_m \to \{y^*\}$, $z_b, e_n, h_m \to \{a^*\}, z_b, e_n, h_m \to \{v^*\}$, которые ставят каждому элементу (z_b, e_n, h_m) трехмерного множества «класс ОИТ – вид информации – условия эксплуатации» $\{E, Z, H\}$ в соответствие некоторые элементы y_i, o_j, v_k множеств *Y, O, V* соответственно, образующие подмножества Y^*, O^*, V^*.

Введение в модель ОИТ подмножеств Y^*, O^* и V^* позволяет определить тип объекта оценки [11, 12] и требуемые средства обеспечения безопасности активов в ОИТ на основании анализа рисков с учетом вида обрабатываемой информации для конкретной конфигурации объекта оценки и условий эксплуатации.

Для получения указанных подмножеств введем определение типа объекта оценки.

Типом объекта оценки называется система или продукт информационных технологий установленной конфигурации, работающий с определенным видом информации в определенной среде безопасности.

Подмножество типов ОО определяется неполным декартовым произведением множеств классов ОИТ, видов информации и условий эксплуатации: $T = Z \times E \times H = \{t_\psi = \langle z_b, e_n, h_m \rangle\}$, $\psi = \overline{1, \Psi}, \Psi \le B \times N \times M, b = \overline{1, B}, n = \overline{1, N}, m = \overline{1, M}$. Некоторые комбинации (z_s, e_n, h_m) не образуют тип ОО $t_\psi = \langle z_b, e_n, h_m \rangle$, т. е. выполняется условие $\exists (z_b) \exists (e_n) \exists (h_m) \quad \overline{\exists} (t_\psi) \ (t_\psi = \langle z_b, e_n, h_m \rangle)$, $b = \overline{1, B}$, $n = \overline{1, N}$, $m = \overline{1, M}, \psi = \overline{1, \Psi}$, вследствие того, что ОИТ некоторых конфигураций не могут работать с информацией различной степени важности в различной среде безопасности из-за невозможности выполнения требований безопасности.

При формировании подмножества типов ОО в случае наличия в ОИТ информации различной степени важности ее вид определяется наибольшей ценностью, уровнем секретности и т. д. Однако это условие не означает, что для всех видов активов требуется обеспечить одинаковый уровень защищенности.

Каждому элементу t множества типов ОО оценки соответствуют вполне определенные подмножества Y^*, O^*, V^*, т. е. существуют функциональные отношения $Y^* \subset T \times Y$, $O^* \subset T \times O$, $V^* \subset T \times V$. Введение подмножества типов ОО *T* позволяет определить подмножества Y^*, O^*, V^* как совокупность образов, получаемых при отображении подмножества *T* на множества *Y, O* и *V*: $Y^* : T \to Y$, $O^* : T \to O$, $V^* : T \to V$. Подмножества Y_z^*, O_z^*, V_z^* удовлетворяют условиям $Y = \bigcup_{z=1}^{Z} Y_z^*, O = \bigcup_{z=1}^{Z} O_z^*, V = \bigcup_{z=1}^{Z} V_z^*$.

Указанные подмножества определяют множество рисков нанесения ущерба для конкретного типа объекта оценки $R^* = Y^* \times V^* \times O^* = \{r_{c^*} = \langle y_i^*, v_k^*, o_j^* \rangle\}, c^* = \overline{1, C^*}, C^* \le I^* K^* J^*$ и соответствующее ему множество ущербов, наносимых владельцам активов $U^* = R^* \times S = \{u_{c^*}\} = \{\langle r_{c^*}, s_{c^*} \rangle\}, c^* = \overline{1, C^*}$.

Таким образом, адаптация базовой модели к типу объекта оценки заключается в конкретном определении множеств типов угроз, активов, подлежащих защите, и уязвимостей, характерных для оцениваемого объекта и среды безопасности. Это позволяет наиболее точно определить возможные риски и ущербы, наносимые конкретному типу объекта оценки, что предоставляет возможность правильно определять задачи безопасности, предъявлять конкретизированные требования безопасности на их основе, проводить количественную оценку защищенности.

3. Показатели защищенности, основанные на базовой модели ОИТ

3.1. Общая характеристика показателей защищенности

Под *эффективностью обеспечения безопасности активов в ОИТ* (защищенностью ОИТ) будем понимать степень соответствия реализованных мер требованиям безопасности. Показа-

тель эффективности – это мера, характеризующая соответствие реального результата реализации требований безопасности в ОИТ требуемому значению. Разработанная базовая модель ОИТ позволяет определять обобщенные и частные интегральные показатели защищенности без учета средств обеспечения безопасности [6, 8, 13]. Такими показателями являются риски нанесения ущерба и ущерб, наносимый владельцам активов.

Риск нанесения ущерба является безразмерной величиной, характеризующей возможность нанесения ущерба. Ущерб имеет явный физический смысл и может быть как размерной, так и безразмерной величиной в зависимости от его характера. Характер возможного ущерба может быть классифицирован следующим образом [14]:

– моральный и материальный ущерб деловой репутации организации;

– моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;

– материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;

– материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

– материальный (финансовый) ущерб от невозможности выполнения взятых на себя обязательств перед второй стороной (заказчиком, подрядчиком, партнером и т. д.);

– моральный и материальный ущерб от дезорганизации деятельности организации;

– материальный и моральный ущерб от нарушения межгосударственных и международных отношений.

По степени интегрирования элементов безопасности показатели защищенности можно разделить на три группы: обобщенные интегральные показатели, частные интегральные показатели по двум элементам безопасности, частные интегральные показатели по одному элементу безопасности. *Обобщенные интегральные показатели защищенности* основаны на интегрировании всех элементов безопасности: угроз, уязвимостей и активов. Они характеризуют общую степень уязвимости ОИТ и могут использоваться для оценки общей эффективности защиты активов, обоснования и выбора (разработки) варианта СЗИ, оценки допустимости остаточных рисков, сравнения вариантов средств обеспечения безопасности. *Частные интегральные показатели защищенности* характеризуют вклад одного или нескольких (но не всех) элементов безопасности в защищенность ОИТ. Они основаны на интегрировании части элементов безопасности и определяются путем интегрирования по двум или одному элементу безопасности и соответственно характеризуют вклад отдельного элемента безопасности или коррелированного взаимодействия двух элементов безопасности в возможные негативные последствия нарушения информационной безопасности.

В зависимости от направления использования частные интегральные показатели делятся на показатели по функциям и требованиям безопасности и комплексные. *Частные интегральные показатели по функциям безопасности* характеризуют вклад одного или нескольких (но не всех) элементов безопасности в защищенность ОИТ по определенному классу функциональных требований. Они используются для разработки функциональных требований безопасности при проектировании профиля защиты (задания по безопасности) [6], требований к стойкости средств обеспечения безопасности. Для их получения требуется проведение классификации угроз по функциональным требованиям безопасности [15]. *Частные интегральные показатели по требованиям безопасности* характеризуют вклад одного или нескольких (но не всех) элементов безопасности в защищенность активов с одинаковыми требованиями безопасности. Они используются для оценки и ранжирования элементов безопасности (угроз, уязвимостей, активов) [16, 17]. Комплексные частные интегральные показатели – это показатели защищенности по функциям безопасности с учетом требований безопасности.

3.2. Обобщенные интегральные показатели защищенности

В качестве обобщенных интегральных показателей защищенности ОИТ целесообразно использовать:

– *средний и максимально возможный риски* нанесения ущерба владельцам активов от воздействия всех видов угроз без использования средств обеспечения безопасности,

$R_{\text{ср}} = \sum_c r_c P_i = \sum_i \sum_k \sum_j r_{ikj} P_i$, $R_{max} = \sum_c r_c = \sum_i \sum_k \sum_j r_{ikj}$, характеризующие среднюю и максимально возможную незащищенность (степень уязвимости) ОИТ, где P_i – вероятность появления угрозы *i*-го вида (частота повторяемости);

– *средний и максимально возможный ущербы*, наносимые владельцам активов от воздействия всех видов угроз без использования средств обеспечения безопасности, $U_{cp} = \sum_c s_c r_c P_i = \sum_i \sum_k \sum_j u_{ikj} P_i = \sum_i \sum_k \sum_j s_j r_{ikj} P_i$, $U_{max} = \sum_c s_c r_c = \sum_i \sum_k \sum_j u_{ikj} = \sum_i \sum_k \sum_j s_j r_{ikj}$, характеризующие средние и максимально возможные негативные последствия от нарушения безопасности.

3.3. Частные показатели защищенности, интегральные по двум элементам безопасности

В качестве частных интегральных показателей защищенности ОИТ по двум элементам безопасности целесообразно использовать:

– средний и максимально возможный риски нанесения ущерба при реализации угрозы определенного вида через все возможные уязвимости на активы всех типов $R_{cpi} = \sum_k \sum_j r_{ikj} P_i$, $R_{maxi} = \sum_k \sum_j r_{ikj}$, характеризующие *степень и максимальную степень опасности определенной угрозы,* и соответствующие им ущербы $U_{cpi} = \sum_k \sum_j u_{ikj} P_i = \sum_k \sum_j s_j r_{ikj} P_i$, $U_{maxi} = \sum_k \sum_j u_{ikj} = \sum_k \sum_j s_j r_{ikj}$;

– средний и максимальный риски нанесения ущерба от воздействия всех видов угроз через все возможные уязвимости $R_{cpj} = \sum_i \sum_k r_{ikj} P_i$, $R_{maxj} = \sum_i \sum_k r_{ikj}$, характеризующие *незащищенность активов определенного типа,* и соответствующие им ущербы $U_{cpj} = \sum_i \sum_k u_{ikj} P_i = \sum_i \sum_k s_j r_{ikj} P_i$, $U_{maxj} = \sum_i \sum_k u_{ikj} = \sum_i \sum_k s_j r_{ikj}$;

– средний и максимальный риски нанесения ущерба от воздействия всех видов угроз через определенную уязвимость на все виды активов $R_{cpk} = \sum_i \sum_j r_{ikj} P_i$, $R_{max\,k} = \sum_i \sum_j r_{ikj}$, характеризующие *степень и максимальную степень опасности определенной уязвимости*, и соответствующие им ущербы $U_{cpk} = \sum_i \sum_j u_{ikj} P_i = \sum_i \sum_j s_j r_{ikj} P_i$, $U_{maxk} = \sum_i \sum_j u_{ikj} = \sum_i \sum_j s_j r_{ikj}$.

3.4. Частные показатели защищенности, интегральные по одному элементу безопасности

В качестве частных интегральных показателей защищенности ОИТ по одному элементу безопасности целесообразно использовать:

– средний и максимальный риски нанесения ущерба при реализации угрозы определенного вида через все возможные уязвимости на определенную область активов $R_{\text{cpij}} = \sum_k r_{ikj} P_i$, $R_{\max ij} = \sum_k r_{ikj}$, характеризующие *степень и максимальную степень опасности определенной угрозы для определенного типа активов*, и соответствующие им ущербы $U_{cpij} = \sum_k u_{ikj} P_i = \sum_k s_j r_{ikj} P_i$, $U_{maxij} = \sum_k u_{ikj} = \sum_k s_j r_{ikj}$;

– средний и максимальный риски нанесения ущерба от воздействия всех видов угроз через определенную уязвимость на определенную область активов $R_{\text{cpkj}} = \sum_i r_{ikj} P_i$, $R_{max\,kj} = \sum_i r_{ikj}$,

характеризующие *незащищенность активов определенного типа по определенной уязвимости*, и соответствующие им ущербы $U_{cpkj} = \sum_i u_{ikj} P_i = \sum_i s_j r_{ikj} P_i$, $U_{maxkj} = \sum_i u_{ikj} = \sum_i s_j r_{ikj}$;

– средний и максимальный риски нанесения ущерба при реализации угрозы определенного вида через определенную уязвимость $R_{\text{cpik}} = \sum_j r_{ikj} P_i$, $R_{\max ik} = \sum_j r_{ikj}$, характеризующие *степень опасности определенной атаки*, и соответствующие им ущербы $U_{cpik} = \sum_j u_{ikj} P_i = \sum_j s_j r_{ikj} P_i$, $U_{maxik} = \sum_j u_{ikj} = \sum_j s_j r_{ikj}$.

Заключение

Основным методологическим подходом к разработке математических моделей объекта информационных технологий и его системы защиты является подход, основанный на анализе рисков. Базовая модель ОИТ представляется в виде графа взаимодействия трех множеств (угроз информационной безопасности, уязвимостей ОИТ, активов, подлежащих защите от угроз безопасности) и последствий этого взаимодействия (рисков нанесения ущерба и ущербов, наносимых владельцам активов). Данная модель характеризует максимальный риск нанесения ущерба владельцам активов без использования средств обеспечения безопасности. Основными направлениями использования базовой модели являются: разработка функциональных требований безопасности; определение требуемого состава средств обеспечения безопасности; предъявление требований к их стойкости по реализации функциональных требований безопасности; разработка базовой модели системы защиты. Адаптация базовой модели к типу ОИТ заключается в определении конкретных множеств типов угроз, активов, подлежащих защите, и уязвимостей, характерных для оцениваемого объекта.

Список литературы

1. Хоффман Л.Дж. Современные методы защиты информации. – М.: Сов. радио, 1980. – С. 179–182.

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

3. ИСО/МЭК 15408-1. Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Ч. 1.

4. Каминский В.Г. Типовые подходы оценки рисков информационной безопасности // Тр. науч.-техн. конф. «Безопасность информационных технологий». – Пенза, 2004. – Т. 5. – С. 39–48.

5. Анищенко В.В., Криштофик А.М., Стецюренко В.И. Базовая модель объекта информационных технологий и направления ее использования // Доклады БГУИР. Мат. докл. и краткие сообщения II Белорусско-российской науч.-техн. конф. «Технические средства защиты информации». – Минск, 2004. – № 5. – С. 8.

6. Анищенко В.В., Криштофик А.М. Разработка функциональных требований безопасности к высокопроизводительным вычислительным системам на основе анализа рисков // Докл. Междунар. науч. конф. «Суперкомпьютерные системы и их применение. SSA' 2004». Минск, 26–28 октября 2004 г. – Мн.: ОИПИ НАН Беларуси, 2004. – С. 238–243.

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

8. Анищенко В.В., Криштофик А.М. Показатели защищенности информационных систем // Мат. конф. «Обеспечение безопасности информации в информационных системах». Минск, 11 ноября 2004 г. – Мн.: Академия управления при Президенте РБ. – С. 30–33.

9. Departament of the Nevy Automated Information Systems Security Program, USA // www.cs.nps.navy.mil/curricula/tracks/security/AISGuide/navch08.txt.

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

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

12. Анищенко В.В., Криштофик А.М. Разработка перечня типовых объектов оценки суперкомпьютерной системы кластерного уровня // Тез. докл. шестой военно-науч. конф. Военной академии Республики Беларусь. Минск, 25–26 ноября 2003 г. – Мн.: ВА РБ, 2003. – С. 87–88.

13. Криштофик А.М. Комплексные показатели защищенности объекта информатизации без средств обеспечения безопасности // Мат. IX Междунар. науч. конф. «Комплексная защита информации». Раубичи, 1–3 марта 2005 г. – Мн.: ОИПИ НАН Беларуси, 2005. – С. 82–84.

14. Вихорев С.В. Классификация угроз информационной безопасности // http://www2.cnews.ru

15. Сидак А.А. Структура представления модели угроз безопасности при формировании профилей защиты информационных технологий // Докл. 3-й Междунар. конф. «Цифровая обработка сигналов и ее применение. DSPA-2000». Т. 1. – СПб., 2000.

16. Анищенко В.В., Криштофик А.М. Использование комплексного подхода для ранжирования угроз информационной безопасности // Мат. конф. «Обеспечение безопасности информации в информационных системах». Минск, 11 ноября 2004 г. – Мн.: Академия управления при Президенте РБ. – С. 33–36.

17. Анищенко В.В., Криштофик А.М. Комплексный подход к ранжированию уязвимостей информационных систем // Там же. – С. 36–39.

Поступила 14.03.05

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

V.V. Anishchanka, A.M. Krishtophic

A BASIC MODEL OF INFORMATION TECHNOLOGIES OBJECTS

A basic model of an IT object is represented as an interaction graph of the following security elements: threats – vulnerabilities – assets – risks – damages. The security elements characterize an external security environment, a target of evaluation and consequences of the interaction between them without resort to protection mechanisms. The basic model allows the security experts to specify functional security requirements, to design a protection system model, to select and develop proper security functions, to evaluate security properties. The basic model adaptation to a target of evaluation types is carried out with due regard to configuration and categories of assets to be protected. Generalized and special indices of security properties are introduced to provide the means of protection (vulnerabilities) level evaluation without resort to protection mechanisms, and to rank the threats, vulnerabilities and assets.