ИНФОРМАТИКА

2004 июль-сентябрь №3

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 681.324.067

В.В. Анищенко, А.М. Криштофик

МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ АКТИВОВ В ОБЪЕКТАХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Проводится анализ методов оценки эффективности защиты активов в объектах информационных технологий. Вводятся новое определение риска нанесения ущерба владельцам активов и основанные на нем показатели эффективности защиты. Предлагается обобщенная методика оценки эффективности защиты на основе анализа и управления рисками.

Введение

Определение эффективности реализации требований безопасности является одной из ключевых задач обеспечения безопасности активов на всех этапах жизненного цикла объектов информационных технологий (ОИТ). Ее решение связано с разработкой соответствующих методик, методов и средств оценки эффективности защиты активов, которая затруднена рядом объективных факторов, обусловленных сложностью и динамичностью процессов и информационных потоков, существующих в ОИТ, стремительным развитием информационных технологий, хаотичностью возникновения новых видов угроз, приводящих к появлению новых уязвимостей аппаратных и программных средств как в самом объекте информационных технологий, так и в средствах обеспечения безопасности.

Оценка эффективности защиты активов ОИТ и выбор варианта средств обеспечения безопасности определяются выбранными методами их проведения, которые могут существенно различаться [1 - 5].

1. Нормативно-методическая база по вопросам оценки эффективности защиты активов и направления ее развития

Основой для проведения любых работ в области информационной безопасности, в том числе и оценки эффективности защиты, являются международные стандарты ISO 15408 и ISO 17799. Международный стандарт ISO 15408 «Общие критерии оценки безопасности информационных технологий» определяет функциональные требования, предъявляемые к программно-техническим механизмам защиты активов, требования к адекватности их реализации, а также общую методологию оценки с учетом угроз, уязвимостей, активов, рисков нанесения ущерба и выбора контрмер (управления рисками). Международный стандарт ISO 17799 «Практические правила управления информационной безопасностью» определяет вопросы организации и управления безопасностью. При оценке защищенности Общие критерии позволяют оценить уровень защищенности с точки зрения полноты реализованных функциональных требований и надежности их реализации. Международные стандарты определяют базовый уровень информационной безопасности. На этом уровне проводится качественная оценка рисков, для чего разработаны и используются различными организациями методики качественной оценки эффективности защиты активов, такие как COBRA, RA Software Tool.

Однако в последнее время стали широко использоваться методы полного анализа рисков при повышенных требованиях к информационной безопасности. В связи с этим широкое распространение получили 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. Для эффективного анализа и управления информационными рисками разработаны и широко используются количественные международные методики, позволяющие

в той или иной степени провести полный анализ рисков. К таким методикам относятся CRAMM, Risk Watch, MARION, Buddy System, Method Ware.

К настоящему времени разработано большое количество численных методов и критериев оценки эффективности защиты активов.

2. Анализ существующих методов оценки эффективности защиты активов

Существуют различные подходы к оценке защищенности объектов информационных технологий и выбору варианта защиты активов. Условно их можно классифицировать как стоимостные, функциональные и подходы, основанные на анализе рисков.

Таблица 1

Стоимостные показатели защищенности активов

Показатель защищенности		Обозначения
Наименование	Выражение	
Стоимость возможных потерь	$R = \sum_{i=1}^{I} C_i P_i$	I – количество защищаемых ресурсов; C_i – стоимость i-го ресурса; P_i – пиковая вероятность доступа к i-му ресурсу
Стоимостный интегральный показатель	$W = Q_\Sigma / C_\Sigma$	Q_Σ – суммарный полезный эффект по обеспечению безопасности ОИТ; C_Σ – суммарные затраты на разработку и эксплуатацию СЗИ
Коэффициент стоимости	$Z = \delta C / C$	δC – относительные затраты дополнительных ресурсов на защиту основных ресурсов C
Коэффициент безопасности	$C_л = \sum_{i=1}^{N} k_i \frac{U_{1i}}{S_i + U_{2i}}$, $\sum_{i=1}^{N} k_i = 1$	U_{1i} – предотвращенный ущерб по i-й составляющей безопасности; U_{2i} – понесенный ущерб по i-й составляющей безопасности; Si – затраты на реализацию мер по предотвращению ущерба по i-й составляющей безопасности; k_i – удельный вес значимости критериев; N – количество составляющих безопасности
Рентабельность защиты	$r_0 = Q_0 - B_0 / R_0$	Q_0 – мера эффективности защиты; B_0 – стоимость защиты; R_0 – максимальный ущерб от реализации угроз
Величина риска	$R = R_0(1 - Q_0)$	Q_0 – мера эффективности защиты; R_0 – максимальный ущерб от реализации угроз
Величина общих потерь	$R = R_0(1 - Q_0) + B_0$	Q_0 – мера эффективности защиты; B_0 – стоимость защиты; R_0 – максимальный ущерб от реализации угроз
Потенциальный ущерб от воздействия угроз безопасности	$Э = \frac{C_0 - U}{C_0 + C_{сзи}}$	C_0 – стоимость объектов компьютерных систем; $C_{сзи}$ – стоимость средств защиты информации; U – ущерб от нарушения информационной безопасности при наличии СЗИ
Общая стоимость системы защиты	$C = \sum_{f=1}^{F} \sum_{j \in B_f} \sum_{m \in N_j^f} c_{jm} x_{jm}$	C_{jm} – стоимость использования m-го средства на j-м рубеже; $X_{jm}=\{0,1\}$ – m-е средство не используется, используется на j-м рубеже защиты; F – число возможных целей злоумышленников; B_f – множество номеров угроз, реализуемых при достижении f-й цели; N_j^f – множество номеров СЗИ для противодействия f-й цели на j-м рубеже защиты
Средний объем потерь от деятельности злоумышленника при достижении им всех целей	$C = \sum_{f=1}^{F} \sum_{l=1}^{K_f} \sum_{j \in B_f} P_j^f(l) c_{jf}$	$P_j^f(l)$ – вероятность нахождения системы в состоянии S_j на l-м шаге; C_{jf} – объем потерь системы при реализации злоумышленником j-й угрозы для достижения f-й цели; F – число возможных целей злоумышленников; K_f – число попыток нарушений

Первый подход основан на использовании стоимостных показателей, характеризующихся стоимостью активов, затратами на создание и эксплуатацию ОИТ и средств обеспечения безо-

пасности, затратами на реализацию угроз безопасности в различном сочетании (табл. 1) [6 – 11]. Основным недостатком данного подхода является отсутствие связи показателей защищенности с характеристиками внутренних и внешних факторов и свойств ОИТ, влияющих на обеспечение безопасности активов.

Второй подход основан на использовании одного из свойств защищенности ОИТ в качестве показателя эффективности защиты активов (табл. 2) [7, 12 – 18]. Эти показатели более полно характеризуют защищенность ОИТ по сравнению с показателями, основанными на стоимостном подходе, так как учитывают некоторые характеристики внутренних и внешних факторов и свойств ОИТ, влияющих на обеспечение безопасности активов. Общим недостатком обоих подходов является их несоответствие требованиям критериев оценки безопасности информационных технологий.

Третий подход основан на анализе рисков от воздействия угроз активам и выборе соответствующих контрмер, снижающих риски до допустимых пределов (табл. 3) [1, 19 – 26]. Он является наиболее распространенным, поскольку позволяет оценить возможный ущерб, наносимый владельцу ОИТ, основывается на существующих стандартах в данной области (Общих критериях) и является основным методом правильного определения требований безопасности.

Существует четыре метода оценки эффективности защиты активов в ОИТ, основанных на анализе рисков [1 – 3].

Первый метод (*базовый*) основан на использовании стандартов информационной безопасности. Стандарты определяют некоторый унифицированный (базовый) набор функциональных и гарантийных требований безопасности для широкого класса типовых ОИТ в зависимости от уровня защищенности (уровня гарантии оценки), который необходимо обеспечить, назначения и принадлежности ОИТ. Требуется правильно оценить набор требований безопасности, соответствие которым необходимо обеспечить для данного объекта оценки (ОО), а также выбрать (разработать) методику, позволяющую оценить это соответствие. Из-за своей простоты и надежности данный метод является наиболее распространенным на практике. Он позволяет при минимальных ресурсах делать обоснованные выводы о состоянии ОИТ. Недостатком данного метода является возможность завышения либо занижения требований по обеспечению безопасности, а также отсутствие методик оценки. Средства защиты, определяемые посредством данного метода, как правило, реализуются с помощью штатных средств защиты информации (СЗИ), предоставляемых общесистемным или специальным программным обеспечением, а также другими средствами, предоставляемыми специализированными организациями и специфицируемыми в специальных каталогах.

Второй метод (*детальный анализ рисков*) базируется на анализе рисков. Он предполагает систематический анализ исходных данных для конкретного ОО с целью оценки рисков нарушения безопасности ОИТ и обоснованного выбора средств защиты, соответствующих заданным требованиям. При этом, как правило, оценивается несколько вариантов защиты активов по критерию «эффективность / стоимость». Данный метод позволяет на основе системного подхода, всестороннего анализа исходных данных и требований дифференцированно для каждого ОИТ осуществить выбор требуемого варианта СЗИ и оценить его защищенность. Полученные с помощью данного метода результаты существенно облегчают сопровождение и модернизацию ОИТ. Недостатками метода являются его высокая ресурсоемкость и, как следствие, высокая цена реализации. Он требует максимальных затрат времени и усилий, а также проведения экспертизы для получения наилучших результатов.

Третий метод (*экспертный*) основан на проведении неформального, прагматического анализа рисков. Он не является систематическим или структурированным, а основан на знаниях и опыте экспертов, вследствие чего имеет ряд недостатков (потенциальная субъективность, отсутствие инструментария и формализованных спецификаций, трудности в сопровождении и т. д.). Как правило, данный метод реализуется табличными или матричными способами с использованием рангов (рейтингов, весов) исходных данных. Он обычно не требует много ресурсов. Не являясь эффективным для анализа рисков, данный метод довольно часто используется в теории и на практике, поскольку реализация метода детального анализа рисков в достаточной степени не разработана.

Таблица 2

Функциональные показатели защищенности

Показатель защищенности		Обозначения
Наименование	Выражение	
Степень защищенности	$\eta(t)=\prod_{i=1}^{I}\{1-K_i(t)P_i(t)\}$	I – количество угроз; $K_i(t)$ – коэффициент опасности угрозы; $P_i(t)$ – вероятность реализации угрозы
Вероятность обеспечения безопасности информации	$P_{\text{б}}(t,Z)=\sum_{s=1}^{4}P_s(t,Z)$	$P_s(t,Z)$ – вероятность принятия ОО s-го состояния, при котором обеспечивается защита активов при Z-м варианте зашиты
Вероятность безошибочной работы	$P(t)=\prod_{i=1}^{I}\{1-P_i(t)\}$	I – количество угроз; $P_i(t)$ – вероятность реализации угрозы
Функциональная стойкость	$S=\sum_{h}\frac{n_h}{N}$	n_h – количество угроз, блокируемых функциональными компонентами; N – общее количество угроз; h – число функциональных компонент
Вероятность защиты информации	$P_{\text{э}}=\sum_{r=1}^{R}P_r=\sum_{r=1}^{R}\prod_{l=1}^{L}\prod_{x=1}^{X}p_{rlx}\beta_{lx}\alpha_l$	p_{rlx} – вероятность x–го события в l-й зоне при осуществлении r-й функции защиты; β_{lx} – коэффициент важности x-го события в l-й зоне; α_l – коэффициент важности защиты информации в l-й зоне
Функционально-временной интегральный показатель	$W_{\text{э}}=N_t/N_{\Sigma t}$	N_t – число успешных атак за время t; $N_{\Sigma t}$ – общее число атак за то же время
Вероятность достижения требуемого результата	$W(n)=P[r_n \ r_{mp}]=1-F_n(r_{mp})$	$F_n(r_{mp})$ – функция распределения случайного результата $r(n)$ реализации требований безопасности для n-го способа реализации; r_{mp} – желаемый результат требований безопасности
Рейтинг защищенности системы	$R_s=\sum_{i=1}^{I}z_i=\sum_{i=1}^{I}P_j m_{ij}$	P_j – вероятность отражения угрозы на j-м эшелоне защиты; m_{ij} – рейтинг стойкости механизма защиты i на j-м эшелоне защиты
Рейтинг защиты	$R_M=\sqrt{\sum_{i=1}^{I}(s_i P_i)^2}$	s_i – рейтинг стойкости i-го механизма защиты; P_i – вероятность воздействия угрозы
Вероятность реализации целевой функции	$P=\frac{1}{K}\sum_{k=1}^{K}\sqrt{\sum_{j=1}^{J}\left(w_b^k\left(\prod_{i=1}^{I}P_{ij}^k\right)^2\right)}$	$P_{ij}^{\ k}$ – вероятность правильного выполнения i-го операнда j-й ветви k-й реализации целевой функции; K – число реализаций целевой функции; $w_b^{\ k}$ – коэффициент, учитывающий тип аппаратно-программного комплекта для реализации k-й целевой функции
Вероятность реализации всех целей злоумышленником	$P^p=\prod_{f=1}^{F}\left(1-\prod_{l=1}^{K_f}\left[1-\sum_{j\in B_f}P_j^f(l)\right]\right)$	$P_j^f(l)$ – вероятность нахождения системы в состоянии S_j на l-м шаге; F – число возможных целей злоумышленников; K_f – число попыток нарушений
Вероятность успешного противодействия системы достижению всех целей злоумышленником	$P=\prod_{f=1}^{F}\left(1-\prod_{l=1}^{K_f}\sum_{j\in B_f}P_j^f(l)\right)$	$P_j^f(l)$ – вероятность нахождения системы в состоянии S_j на l-м шаге; F – число возможных целей злоумышленников; K_f – число попыток нарушений

Таблица 3

Критерии эффективности защиты активов с использованием оценки риска

Риск	Показатель эффективности	Примечание
Риск от воздействия атаки $W_i = (P_i + K) - (P_c + P_{cy})$	Интегральный риск $W = \sum_i W_i$	P_i – вероятность осуществления атаки; K – критичность сетевого ресурса; P_c – эффективность СЗИ системного уровня; P_{cy} – эффективность СЗИ сетевого уровня
Риск от воздействия атаки $W_i = P_i U$	Интегральный риск $W = \sum_i W_i$	P_i – вероятность осуществления атаки; U – ущерб от атаки i-го вида
Риск от воздействия угрозы $W_i = P_i U(1 - P_{см})$	Защищенность ОИТ $W = 1 / \sum_i W_i$	P_i – вероятность появления угрозы; U – ущерб от угрозы i-го вида; $P_{см}$ – вероятность преодоления механизма защиты
Риск от реализации угрозы $W_i = RP_i$	Защищенность ОИТ $W = \sum_i W_i$	R – показатель негативного воздействия (ресурса); P_i – вероятность реализации угрозы
Риск от воздействия угрозы $W_i = \sum_j C_{ji} P_{ji} P_i$	Средний риск $W = \sum_j \sum_i C_{ji} P_{ji} P_i$	C_{ji} – потери от воздействия угрозы i-го вида при принятии ОИТ j-го состояния; P_{ji} – вероятность принятия ОИТ j-го состояния при воздействии угрозы i-го вида; P_i – вероятность появления угрозы i-го вида
Риск от реализации угрозы $R = \frac{1}{n} \sum_{i=1}^{n} (t_i \times v_i)$	Процент снижения риска за счет контрмер $(R\%) = \left(\frac{nR - R_m}{nR} \right) 100\%;$ $R_m = \sum_{i=1}^{n} (t_i \times v_i \times M_i);$ $M_i = \prod_{i=1}^{k} m_i$	t_i – балльная оценка угрозы; v_i – балльная оценка уязвимости данного актива на действие i-й угрозы; n – число угроз; M_i – коэффициент ослабления i-й угрозы за счет всех контрмер; m_i – коэффициент ослабления i-й угрозы за счет контрмеры; k – общее число контрмер против i-й угрозы .
Риск нанесения ущерба $R_{ij} = \frac{C_i P_j}{U}$	Суммарный риск нанесения ущерба $R = \sum_{i=1}^{I} \sum_{j=1}^{J} R_{ij}$	Ci – стоимость i-го ресурса; P_j – вероятность j-й угрозы; U – величина уязвимости

-

Четвертый метод (*комбинированный*) предполагает использование (комбинирование) в различных сочетаниях основного метода, метода детального анализа рисков и экспертного метода [2, 23].

Применение комбинированного метода целесообразно в том случае, когда требуются повышенные требования к режиму информационной безопасности, т. е. в случаях, когда нарушение информационной безопасности чревато тяжелыми последствиями и базовый уровень информационной безопасности является недостаточным.

Выбор одного из рассмотренных методов зависит от требований безопасности, оценки собственниками ценности (важности) своих активов, сложности ОИТ и возможных последствий нарушения режима информационной безопасности. Однако все разработанные критерии оценки эффективности защиты активов с использованием оценки риска не связаны в полной мере ни с одним из рассмотренных методов.

3. Риск нанесения ущерба владельцам активов

Большое разнообразие методов и критериев оценки защищенности ОИТ, основанных на анализе рисков, обусловлено тем, что, несмотря на широкое использование этих методов, понятие риска в области безопасности информационных технологий до сих пор не имеет единого

общепризнанного определения. Так, в терминологическом словаре Центра компьютерной безопасности США (NCSC) приведены два определения риска безопасности [27]:

- ожидаемые потери, обусловленные установленными угрозами или воздействиями этих угроз, выраженные в терминах уязвимых мест системы и прочности защиты или действий агентов угроз;

- вероятность, что определенная угроза будет реализовываться через данное уязвимое место системы.

Первое определение не содержит какой-либо конкретной метрики риска, допускает качественную его оценку и обычно предполагает выбор подлежащих защите активов, выявление угроз этим активам, уязвимых мест реализации этих угроз, а также проверку адекватности средств защиты установленным угрозам. Такой подход называется «доверительным методом оценки рисков» [28].

Второе определение предполагает использование вероятностной (количественной) меры риска. Большинство количественных методов оценки риска («обычных» по зарубежной терминологии) по своей сути являются расширением качественных методов с добавлением балльных, вероятностных либо экспертных оценок уровня угроз и уязвимостей, а в некоторых случаях и активов.

В глоссарии терминов по информационной безопасности приводится восемь определений риска, коррелированных в той или иной степени с приведенными выше, и 13 определений угроз, взятых из зарубежных источников [29].

Обобщая все определения риска информационной безопасности, а также методы оценки риска, введем новое определение риска нанесения ущерба владельцам активов и уровня защищенности ОИТ.

Риск *– это мера, определяющая возможность нанесения ущерба владельцу активов посредством реализации угроз безопасности через установленные уязвимости на определенные области активов.*

Уровень защищенности ОИТ *– это мера, определяющая возможность предотвращения ущерба, наносимого владельцу активов, посредством использования данного комплекса средств обеспечения безопасности активов при реализации угроз через установленные уязвимости на определенные области активов*.

Новые определения позволяют:

- использовать как качественные, так и количественные методы оценки риска при любом априорно известном и доступном для исследователя числе характеристик угроз, уязвимостей, средств обеспечения безопасности и активов, а также объединять качественные и количественные показатели в интегральный показатель защищенности ОИТ;

- определять ущерб, наносимый владельцам для любых видов активов: *ущерб = риск* $\times$ *ценность активов*;

- определять уровень защищенности ОИТ: *уровень защищенности = максимально возможный риск – риск.*

- определять ущерб, предотвращенный за счет использования КСБО: *предотвращенный ущерб = уровень защищенности* $\times$ *ценность активов.*

Введенные показатели в полной мере характеризуют защищенность ОИТ и могут использоваться для оценки эффективности защиты активов в ОИТ.

4. Обобщенная методика оценки защищенности ОИТ

Проведенный анализ методов оценки защищенности ОИТ, введенные понятия и требования стандартов в области защиты информационных технологий позволяют сделать вывод о том, что для оценки защищенности активов целесообразно использовать обобщенную методику (рис.). Она несколько расширяет концепцию управления рисками, разработанную Национальным институтом стандартов США (NIST) в стандарте NIST 800-30, за счет оценки остаточного риска, который был предложен (но не определен) в диаграмме анализа рисков стандарта Cobit «Контрольные объекты для информационных и смежных технологий», разработанного Ассоциацией аудита и контроля информационных систем (ISACA).

Методика определения эффективности защиты активов в ОИТ на основе оценивания рисков в соответствии с критериями оценки безопасности информационных технологий включает решение следующих задач: *определение исходных данных, анализ рисков, управление рисками, оценка защищенности.*

Определение исходных данных включает определение политики безопасности и предположения об объекте и среде; определение активов, требующих защиты.

Второй задачей является *анализ рисков*. Степень риска зависит от показателей ценности и важности активов, опасности угроз и вероятностей их реализации, показателей опасности уязвимостей, показателей опасности атаки, характеристик существующих и планируемых к внедрению средств обеспечения безопасности, которые уменьшают уязвимости, вероятности возникновения угроз и негативные воздействия на активы.

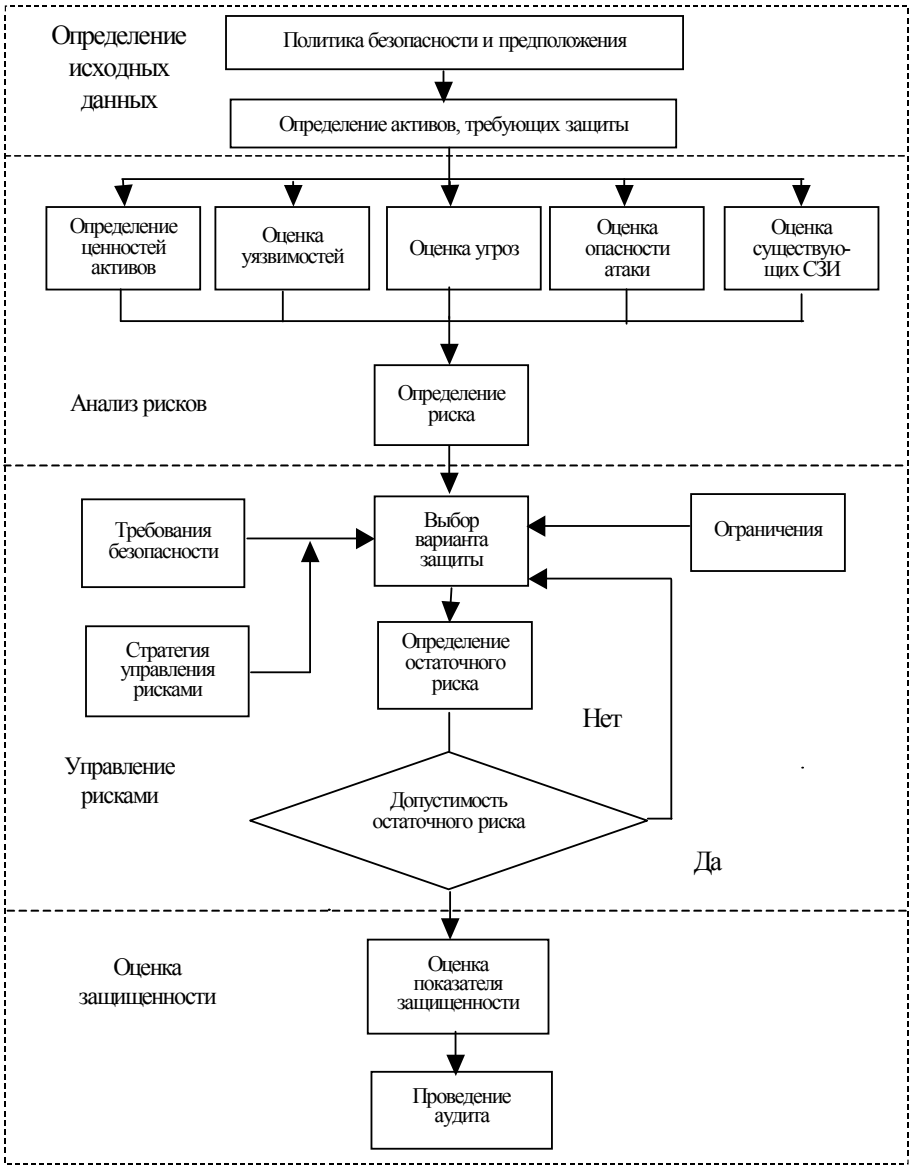

Рис. Методика оценки защищенности ОИТ

Процесс оценивания рисков включает, как правило, несколько этапов: идентификацию активов, подлежащих защите, и оценивание их количественных или качественных характеристик или определение потенциального негативного воздействия на владельцев активов; оценивание угроз, определение наиболее опасных; оценивание уязвимостей, определение наиболее опасных; оценивание опасности атак, определение наиболее опасных; оценивание существую-

щих и предполагаемых средств обеспечения информационной безопасности; оценивание рисков.

Задача *управления рисками* включает выбор и обоснование выбора контрмер, позволяющих снизить величины рисков до приемлемых.

При выборе варианта средств обеспечения безопасности активов, в зависимости от разработанной стратегии управления рисками, определяются подходы к снижению риска, такие как уменьшение риска, уклонение от риска, изменение характера риска, принятие риска [30].

Управление рисками включает в себя также 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 возможность (достоверность) причинения ущерба.

Снижение рисков за счет использования контрмер может осуществляться различными способами [21]:

- уменьшением вероятностей осуществления угроз безопасности;
- ликвидацией уязвимостей или уменьшением их величин;
- уменьшением величины возможного ущерба;
- восстановлением ресурсов, которым был нанесен ущерб;
- выявлением атак и других нарушений безопасности.

Выбор варианта защиты активов осуществляется на основании результатов оценки рисков с учетом требований безопасности и существующих стоимостных и других ограничений. Основой для выбора варианта защиты активов является общесистемный критерий «эффективность / стоимость». С позиций системного подхода, экономической целесообразности и существующих ограничений использование указанного критерия означает выбор такого варианта средств безопасности, который обеспечивает:

- минимум остаточного риска при существующих ограничениях на стоимость средств обеспечения безопасности активов

$$z = \underset{z}{arg\ min}\, R_z = \sum_{i=1}^{N} a_i r_{iz}, C_z = \sum_{i=1}^{N} C_{iz} \le C_0 ;$$

- минимум остаточного риска при существующих ограничениях на величину остаточного риска (приемлемость остаточного риска)

$$\mathrm{z} = \underset{\mathrm{z}}{\mathrm{argmin}}\, R_z = \sum_{i=1}^{N} a_i r_{iz}, \ R \le R_0, \ C_z = \sum_{i=1}^{N} C_{iz} \le C_a ;$$

- минимум стоимости средств обеспечения безопасности при существующих ограничениях на величину остаточного риска

$$z = \underset{z}{arg\ min}\, C_z = \sum_{i=1}^{N} C_{iz}, C_z \le C_a , R_z \le R_0 ,$$

где R_z – значения остаточного риска при z-м варианте средств обеспечения безопасности;

C_0, R_0 – ограничения на стоимость средств обеспечения безопасности активов и величину остаточного риска соответственно;

C_z – стоимость средств обеспечения безопасности активов при z-м варианте средств обеспечения безопасности;

C_{iz} – стоимость средств обеспечения безопасности по i-му частному свойству защиты;

C_a – стоимость активов, подлежащих защите;

r_{iz} – значения остаточного риска по i-му частному свойству защиты при использовании z -го варианта средств обеспечения безопасности;

N – количество частных свойств защиты;

a_i – весовые коэффициенты.

Однако необходимо иметь в виду, что минимум указанных критериев достигается не для всех значений существующих ограничений на стоимость средств обеспечения безопасности и величину остаточного риска.

С учетом характеристик средств обеспечения безопасности определяется остаточный риск, который сравнивается с допустимым значением. При недопустимости остаточного риска производится повторное задание требований безопасности и выбор варианта средств защиты информации, которые определяют остаточный риск. Если величина остаточного риска допустима, то производится оценка защищенности ОИТ.

Оценка защищенности ОИТ производится в два этапа: оценка показателей защищенности на основе анализа рисков и проведение аудита.

Отличительной особенностью и достоинством данного подхода является необходимость оценки рисков нанесения ущерба владельцам активов ОИТ до разработки и внедрения средств обеспечения безопасности. На основании анализа рисков принимаются контрмеры для их снижения до приемлемой величины. По величинам риска и остаточного риска предъявляются требования к стойкости средств обеспечения безопасности. Показатель защищенности ОИТ в этом случае является функцией остаточного риска в соответствии с введенным определением риска.

Заключение

Рассмотрена важная в методическом и прикладном плане задача оценки эффективности защиты активов, которая возникла в связи с отсутствием математического и методического аппаратов оценки обеспечения безопасности в соответствии с Общими критериями. Анализ методов и критериев оценки эффективности защиты активов ОИТ показал отсутствие взаимосвязи между ними. Основным показателем эффективности защиты активов является риск нанесения ущерба. Для оценки защищенности необходимо использовать комбинированные методы анализа рисков на основе введенных показателей эффективности защиты активов. Анализ рисков в соответствии с предложенной обобщенной методикой необходимо проводить в два этапа: без средств защиты и после их включения в состав ОИТ. Такой подход в наиболее полной мере соответствует требованиям Общих критериев и позволяет оценить эффективность средств защиты и их вклад в обеспечение безопасности активов. Однако реализация обобщенной методики требует разработки соответствующих моделей и математического аппарата.

Список литературы

1. Симонов С.В. Методология анализа рисков в информационных системах // Защита информации. Конфидент. – 2001. – №1. – С.72-76.

2. Майданский И.С. Методология построения системы управления безопасностью ИТ. http://ivmai.chat.ru/papers/net

3. Майданский И.С., Сухомлин В.А. Методика и средства автоматизации проектирования политики безопасности информационных технологий. http://ivmai.chat.ru/papers/net .

4. Баутов А. Экономический взгляд на проблемы информационной безопасности. http://www.morepc.ru.

5. Морозов А. Выбор рациональной структуры средств защиты информации в АСУ. http://kiev-security.org.ua.

6. Амерханова Ю.Р., Струков В.И. Система оценки уровня затрат по защите информации на предприятии. http://www.tsure.ru/University/Faculties/Fib/bit/sections/ cjnferenses / sem2001 /58.htm.

7. Давыдов Г.В., Шамгин Ю.В. Функциональные требования безопасности класса FCO «Связь». Показатели и критерии оценки эффективности // Комплексная защита информации: Сб. мат. VI Междунар. конф., 26 февраля – 1марта 2002 г., Суздаль. – Минск, 2002. – С. 54 - 56.

8. Васильев В.И., Бабкова Т.О. Динамические сетевые модели для оценки защищенности объектов информатизации // Информация и безопасность. Вып. 2. – Воронеж: Воронежский гос. техн. ун-т, 2002. – С. 190-193.

9. Есиков О.В., Кислицин А.С. Применение теории марковских цепей для построения модели оптимизации комплексов средств защиты современных систем передачи и обработки данных // Докл. III Междунар. конф. «Цифровая обработка сигналов и ее применение (DSPA-2000). Т. 1. – М.: Ин-т проблем управления РАН, 2000. – С. 33-35.

10. 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.

11. Морозов А. Концепция безопасности – математический анализ. http: // kiev-security. org.ua/box/2/130.shtml/.

12. Об одном алгоритме оптимизации выбора целесообразного состава мер и средств защиты информации на объекте информатизации / А.В. Жижелев, Ю.К. Язов, Р.В. Батищев, Н.М. Талтынова // Информация и безопасность. Вып. 1. – Воронеж: Воронежский гос. техн. ун-т, 2002. – С. 25-29.

13. Анищенко В.В., Стецюренко В.И. Подход к оценке эффективности реализации требований безопасности класса «Идентификация и аутентификация» // Комплексная защита информации: Сб. мат. VI междунар. конф., 26 февраля – 1 марта 2002 г., Суздаль. – Минск, 2002. – С. 37-39.

14. Лахтиков А.И., Сычев М.П. Вероятностный подход к оценке эффективности управления безопасностью информации в локальных информационных сетях // Вопросы защиты информации. – № 1–2. – М., 1997. – С. 14-16.

15. Анищенко В.В., Криштофик А.М. Об одном из подходов к оценке вероятностей реализации угроз безопасности информации // Комплексная защита информации: Сб. тез. докл. VII Междунар. конф., 25-27 февраля 2003 г., Раубичи. – Минск, 2003. – С. 39-41.

16. Нестеров С.В. Модель выбора функций и задач защиты информации в автоматизированных системах обработки данных // Вопросы защиты информации. – №3. – М., 1996. – С. 16-20.

17. Шевченко В.В. Метод оценки защищенности продуктов информационных технологий на основании количественных показателей //Вопросы информационной безопасности: Сб. науч. тр. Вып. 1. – Мн.: ОИПИ НАН Беларуси, 2002. – С. 89-94.

18. Особенности анализа информационного конфликта в автоматизированных системах / С.Д. Буслов, В.А. Павлов, Р.В. Павлов, Н.Н. Толстых //Информация и безопасность. – Вып. 2. – Воронеж: Воронежский гос. техн. ун-т, 2002. – С. 167-170.

19. Осовецкий Л.Г., Шевченко В.В. Метод интегральной оценки защищенности продуктов информационных технологий // Комплексная защита информации: Сб. мат. VI Междунар. конф., 26 февраля – 1марта 2002 г., Суздаль. – Минск, 2002. – С. 99-101.

20. Анищенко В.В., Криштофик А.М. Некоторые подходы к построению матрицы потерь при оценке эффективности средств защиты информации // Комплексная защита информации: Сб. тез. докл. VII Междунар. конф. 25-27 февраля 2003 г., Раубичи. – Минск, 2003. – С. 36-38.

21. Астахов А. Актуальные вопросы выявления сетевых атак. http://www.cobit.ru/ security/Pubs/ Pub2_AAM_ID.htm

22. Морозов А. Создание политики информационной безопасности. http://kiev-security.org.ua

23. Астахов А. Аудит безопасности информационных систем. http://www/ networkdoc.ru

24. Анищенко В.В., Криштофик А.М. Вероятностный подход к оценке эффективности средств защиты информации // Вопросы информационной безопасности: Сб. науч. тр. Вып.1. – Мн.: ОИПИ НАН Беларуси, 2002. – С. 73-84.

25. Давыдов Г.В., Шамгин Ю.В. Оценка рисков безопасности при обеспечении защищенности систем информационных технологий // Управление защитой информации. – № 3. – Минск – Москва, 2001. – С. 262-264.

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

27. NCSC-TG-004 (Aqua Book) Glossary of Computer Security Terms (Version 1, 0/21/88). www.radium.ncsc.mil/tpep/library/rainbow/index.html.

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

29. Глоссарий терминов по информационной безопасности. http://www.garlic.com/-lynn/secure.htm.

30. Симонов С. Анализ рисков, управление рисками // Jet Info. – № 1 (68). – М., 1999.

Поступила 06.04.04

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

U.V. Anishchanka, A.M. Krishtophic

METHODS OF EVALUATING THE EFFECTIVENESS OF PROTECTING THE ASSETS IN INFORMATION TECHNOLOGY OBJECTS

An analysis of the methods and criteria of evaluating the effectiveness of protecting information technology assets has shown that the risk of damage poses as the principal criterion of effectiveness in providing the security of the assets. It is advisable to use the combination methods of risks analysis, based on the assets' protection efficiency indices introduced. In conformity with the generalized methods, the risks analysis has to be performed in two stages: prior to designing (selecting) the security means, and following their introduction. This approach will meet all the requirements of the Common Criteria, and will enable to set the security requirements in a scientifically substantiated manner, as well as to perform the elaboration (selection) of security means, to evaluate their effectiveness and contribution into the protection of assets with sufficient accuracy.