УДК 004.056.53

ПРАКТИЧЕСКИЕ АСПЕКТЫ ОЦЕНИВАНИЯ РИСКОВ РЕАЛИЗАЦИИ УГРОЗ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Александр Архипов, Андрей Скиба

Одна из насущных проблем исследования и эксплуатации систем защиты информации (СЗИ) – оценивание обобщенного показателя защищенности СЗИ, в качестве которого часто выступает так называемый интегральный риск. Это скалярный показатель, являющийся отображением набора частных рисков (рисков атак, рисков угроз, рисков уязвимостей отдельных элементов информационных систем (ИС)). В статье сформулированы условия корректного отображения частных рисков в интегральный. Рассмотрены механизмы возникновения рисков, в частности, процессы развития деструктивных последствий реализации угроз и образования потерь. Исследованы проблемы, возникающие при оценивании вероятностного параметра риска и определения уровня потерь в случае множественных угроз. Предложена методика приоритезации информационных активов ИС по степени их уязвимости.

Ключевые слова: *риск, интегральный (обобщенный) риск, суммарный риск, риск атак (угроз), механизм возникновения риска, вероятностный параметр риска.*

Введение. Одним из важных показателей уровня безопасности информации в информационной системе (ИС) организации, позволяющем в совокупности учесть влияние всего множества актуальных для данной ИС угроз, является обобщенный риск *R*, называемый также интегральным риском. Нахождение обобщенного риска – завершающий этап процесса анализа и оценивания рисков (АОР), в ходе которого результаты АОР, представленные профилем рисков, отображаются в скалярный показатель R. Очевидно, что как структура обобщенного риска, так и процедура его вычисления должны обеспечивать объективность и корректность производимого отображения. Однако корректность именно этих аспектов оценивания рисков часто оказывается под вопросом. Рассмотрим проблемы, возникающие при применении одной из наиболее распространенных форм показателя обобщенного риска, называемой суммарным риском [1,2]:

$$R_{\Sigma} = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} p_i q_i, \qquad (1)$$

где r_i – значение риска, обусловленное возможным влиянием некоторого негативного фактора v_i, вероятность реализации которого – p_i, а q_i – потери организации, возникающие в случае реализации воздействия этого фактора на объект риска, в данном случае – на ИС организации.

Постановка задачи. Логику возникновения и развития негативных воздействий на ИС в общем случае можно описать следующей схемой: **опасности среды функционирования ИС ⇒ воздействие опасных явлений и процессов на элементы ИС ⇒ угрозы информационным активам ИС ⇒ атаки уязвимостей ИС ⇒ потери организации, обусловленные реализацией угроз.**

При этом в ходе АОР рассчитывается три вида рисков: риски атак, реализующих ту или иную угрозу, риски отдельных угроз и обобщенный риск R, обусловленный опасностями среды функционирования ИС (т.е. совместными действиями всей совокупности угроз, генерируемых средой функционирования ИС). Если воспользоваться формулой (1) для расчета риска, связанного с влиянием, некоторой угрозы t_i, которая может быть реализована любой успешной атакой α_j из множества $\mathbf{A}=\{\alpha_j\}$, $j=\overline{1,k_i}$, получим следующее выражение:

$$r_i = \sum_{j=1}^{k_i} \rho_j = \sum_{j=1}^{k_i} p_{aj} q_i = q_i \sum_{j=1}^{k_i} p_{aj}, \qquad (2)$$

где $\rho_j = p_{aj} q_i$ – частный риск, обусловленный успехом атаки α_j, позволяющей реализовать угрозу t_i, используя уязвимость v_j, p_{aj} – вероятность успешного завершения атаки α_j. Соотношение (2) выведено в предположении, что реализация угрозы t_i посредством любой из атак $\{\alpha_j\}$, $j=\overline{1,k_i}$, ведет к одной и той же величине потерь q_i. При этом, учитывая, что для произвольной вероятности p_{aj} справедливо неравенство $0 \le p_{aj} \le 1$, очевидно утверждение:

$$0 \le \sum_{j=1}^{k_i} p_{aj} \le k_i. \qquad (3)$$

С другой стороны, т.к. риск, обусловленный возможной реализацией угрозы t_i, определяется формулой:

$$r_i = q_i p_{ti}, \quad (4)$$

из сопоставления выражений (2) и (4) вытекает равенство:

$$p_{ti} = \sum_{j=1}^{k_i} p_{aj}, \quad (5)$$

из которого, принимая во внимание, что значение вероятностного параметра p_{ti} не может превышать 1, следует ошибочность правого неравенства в утверждении (3). Причину возникновения этого противоречия можно выяснить, описав ситуацию <угроза t_i / атаки > с позиций теории вероятностей.

Обобщение рисков на уровне атак. Пусть $< v_0, v_1, ..., v_{ki} >$ – множество элементарных событий, связанных с возможностью наступления события t_i (реализацией угрозы t_i), причем v_0 - элементарное событие, состоящее в невозможности реализации угрозы t_i, а события $v_1, ..., v_{ki}$ – успешные реализации атак $\alpha_1, ..., \alpha_{ki}$, вектор $P = [p_{a0}, p_{a1}, ..., p_{\alpha ki}]$ составлен из вероятностей соответствующих элементарных событий, а условные вероятности наступления события t_i определены формулами: $p(t_i / v_0) = 0$, $p(t_i / v_j) = 1$, $j = \overline{1, k_i}$. Если множество $< v_0, v_1, ..., v_{ki} >$ представляет полную группу событий (т.е. вероятность $P(v_j \cap v_l) = 0$, $j \neq l$ и $\sum_{j=0}^{k_i} p_{aj} = 1$), то

$$p_{ti} = \sum_{j=0}^{k_i} p_{aj} p(t_i / v_j) = \sum_{j=1}^{k_i} p_{aj}, \quad (6)$$

и, следовательно, в этом случае выражение (2) справедливо: риск, возникающий в результате возможности реализации угрозы t_i, является суммарным риском атак.

Однако в общем случае атаки могут осуществляться совместно (комплексно), в частности, вероятность успешной реализации угрозы t_i путем проведения комплексной атаки выше, чем путем реализации составляющих ее одиночных атак. Поэтому множество $< v_0, v_1, ..., v_{kj} >$ уже не является полной группой и для расчета рисков в этой ситуации в [1,2] рекомендуется трансформировать исходное множество элементарных событий $< v_0, v_1, ..., v_{kj} >$ в множество комплексных событий, составляющих полную группу, рассчитать вероятности полученных комплексных событий (атак), соответствующие им потери, частные риски потерь вследствие реализации комплексных атак и, наконец, риск r_i, связанный с реализацией угрозы t_i и обобщающий частные риски атак.

Для примера, из исходного множества атак $< \alpha_1, \alpha_2 >$, допускающих свое совмещение, формируем полную группу из четырех комплексных событий $< v_1 v_2, v_1 \overline{v_2}, \overline{v_1} v_2, \overline{v_1}\,\overline{v_2} >$, где v_j и $\overline{v_j}$ составляют пару противоположных событий, рассчитываем вероятности этих комплексных событий: $p_{12} = p_{a1} p_{a2}$, $p_{10} = p_{a1}(1 - p_{a2})$, $p_{02} = (1 - p_{a1}) p_{a2}$, $p_{00} = (1 - p_{a1})(1 - p_{a2})$, оцениваем соответствующие значения потерь, полагая, что $q_{12} = q_{10} = q_{02} = q_i$, $q_{00} = 0$. В итоге для угрозы t_i получаем абсолютно корректные соотношения: вероятность реализации угрозы t_i, представленная через вероятности атак, составляет:

$$p_{ti} = p_{12} + p_{10} + p_{20} = 1 - p_{00} = p_{a1} + p_{a2} - p_{a1} p_{a2}, \quad (7)$$

соответственно риск угрозы t_i:

$$r_i = p_{12} q_{12} + p_{10} q_{10} + p_{20} q_{20} = (p_{12} + p_{10} + p_{20})\, q_i = q_i p_{ti}. \quad (8)$$

В общем случае реальные потери, возникающие при реализации каждой из комплексных атак, могут не совпадать друг с другом: $q_{12} \neq q_{10} \neq q_{02} \neq q_i$, $q_{00} = 0$. Тогда для угрозы t_i получаем риск $r_i = p_{12} q_{12} + p_{10} q_{10} + p_{20} q_{20}$, и далее из выражения (4) находим величину совокупных потерь, обусловленные реализацией угрозы t_i:

$$q_i = r_i / p_{ti}. \quad (9)$$

Обобщение рисков на уровне угроз. При существовании в ИС группы угроз $T = \{t_i\}$, $i = \overline{1, n}$, для которых условие несовместности обычно не выполняется, методика расчета обобщенного риска R (риск, обусловленный существованием всевозможных опасностей, генерирующих все угрозы, действующие в среде функционирования ИС) практически ничем не отличается от уже рассмотренной методики обобщения рисков атак. В частности, из исходного множества угроз T формируется множество комплексных угроз, составляющих полную группу событий [1], объем которой N в общем случае определяется по формуле: $N = 2^n$. Исходя из заданного набора априорных вероятностей $\{p_{ti}\}$,

$i=\overline{1,n}$ реализации каждой из множества исходных угроз $T=\{t_i\}$, рассчитываются вероятности реализации комплексных угроз P_{tl}, $l=\overline{1,N}$; из множества исходных потерь $\{q_i\}$, $i=\overline{1,n}$, обусловленных реализациями соответствующих угроз t_i, формируется множество совокупных потерь $Q=\{Q_{tl}\}$, $l=\overline{1,N}$, возникающих в результате реализации комплексных угроз [1]. По полученным данным рассчитываются риски R_{tl}, $l=\overline{1,N}$ комплексных угроз, а затем в соответствии с формулой (1) определяется их суммарный риск:

$$R=PQ=R_{\Sigma}=\sum_{l=1}^{N}R_{ti}=\sum_{l=1}^{N}P_{ti}Q_{ti}\,, \qquad (10)$$

являющийся характеристикой, обобщающей частные риски отдельных угроз, т.е. интегральным риском группы угроз $T=\{t_i\}$. Совокупные потери, обусловленные воздействием на ИС существующих в среде ее функционирования разнообразных опасностей, генерирующих множество угроз $T=\{t_i\}$, $i=\overline{1,n}$, определим из выражению (10):

$$Q=R/P=R/(1-P_{t0}), \qquad (11)$$

где $P_{t0}=\prod_{i=1}^{n}(1-p_{ti})$ - вероятность того, что в ИС отсутствует влияние каких либо опасностей.

Приведенные выше материалы содержат рекомендации общеметодологического характера, суть которых сводится к формулированию требований, в рамках которых применение формулы суммарного риска (1) приводит к получению корректного результата. Как правило, на практике реализация этих требований сводится к необходимости трансформации исходной рисковой ситуации, сложившейся в результате действия совокупности реальных деструктивных случайных совместных событий, к рисковой ситуации, описываемой действием полной группы комплексных случайных событий, формируемых из исходной совокупности реальных. К сожалению, практическое использование этого подхода сопряжено с определенными трудностями. Чаще всего это связано с неопределенностью, появляющейся при анализе деструктивных последствий реализации угроз и оцениванием обусловленной ими величины потерь. Описание, детализация и анализ некоторых из возникающих при этом ситуаций рассмотрен ниже.

Особенности описания и анализа рисковых ситуаций. В общем виде рекомендации по процедуре оценивания информационных рисков, актуальных для деятельности некоторой организации, приводятся в соответствующих стандартах [3,4] и детально проанализированы в [5]. Отмечается, что величина риска определяется уменьшением стоимости (ценности) активов организации, вызванным реализацией информационной угрозы t либо совокупности угроз $T=\{t_i\}$. При этом в общей массе активов организации выделяются две группы: информационные активы *IA* и вторая группа активов *AS*, куда входят все другие активы организации, ценность которых зависит от состояния активов первой группы.

К информационным активам *IA* (активам ИС) обычно относят те элементы ИС, которые непосредственно используются для реализации тех или иных информационных технологий:

– информационные ресурсы *IR* организации – базы данных, файлы данных, системную документацию, руководства пользователям, архивированную информацию и т.д.;

– программное обеспечение: системное, прикладное, инструментальные средства, утилиты;

– физические активы ИС: компьютерное оборудование (процессоры, мониторы, периферийные устройства и т.п.), аппаратуру связи (телефонные станции, маршрутизаторы, модемы и пр.), другое техническое оборудование, сооружения и помещения ИС;

– персонал и сотрудников ИС.

Состав активов AS (другие активы организации) существенно зависит от сферы, в которой функционирует организация, ее финансового состояния, подчиненности и т.д.

В частности, это нематериальные активы: репутация, имидж организации, уровень ее деловой активности. Сюда же следует отнести коммунальные активы: освещение, кондиционирование, обогрев, электропитание. Наконец, это могут быть продукция и услуги, производимые организацией, условия, определяющие выполнения работ организациями-смежниками, поставщиками и многое другое. Перечень активов второй группы может быть достаточно объемным, их отличительной чертой – зависимость стоимости этих активов от последствий реализации угрозы t_i, выражающаяся в:

– снижении уровня деловой активности организации;

– потере/ухудшении репутации организации;

– финансовых потерях;
– перебоях в исполнении деловых операций;
– ухудшении инвестиционного климата;
– возникновении угроз личной безопасности персонала и т.п.

Рассмотрим оценивание риска реализации некоторой угрозы t, ориентированной на поражение конкретного информационного ресурса ir_m. Механизм формирования риска представлен на рис.1. Получить доступ к ресурсу ir_m можно только через те элементы ИС, которые непосредственно используются для транспортировки (передачи), хранения и обработки информации, представленной этим ресурсом, т.е. через информационные активы, в рассматриваемом примере – через ia_1, ia_2, ... ,ia_K. Очевидно, что реализации угрозы t возможно лишь при наличии уязвимостей в этих активах, путем проведения успешных атак, эксплуатирующих имеющиеся уязвимости, причем в общем случае у актива может быть несколько уязвимостей.

Вначале оценим вероятность $p_t(ir_m / ia_k)$ успешной атаки ресурса ir_m через актив ia_k в предположении, что для актива характерны уязвимости, допускающие организацию атак $\alpha_0, \alpha_1, ..., \alpha_{l_s}$, вероятности успешных реализаций которых представлены вектором $P = \left[p_{a0}, p_{a1}, ..., p_{\alpha l_s} \right]$. В этой ситуации вероятность $p_t(ir_m / ia_k)$ определяется формулой:

$$p_t(ir_m / ia_k) = 1 - \prod_{j=1}^{l_s} (1 - p_{aj}). \qquad (12)$$

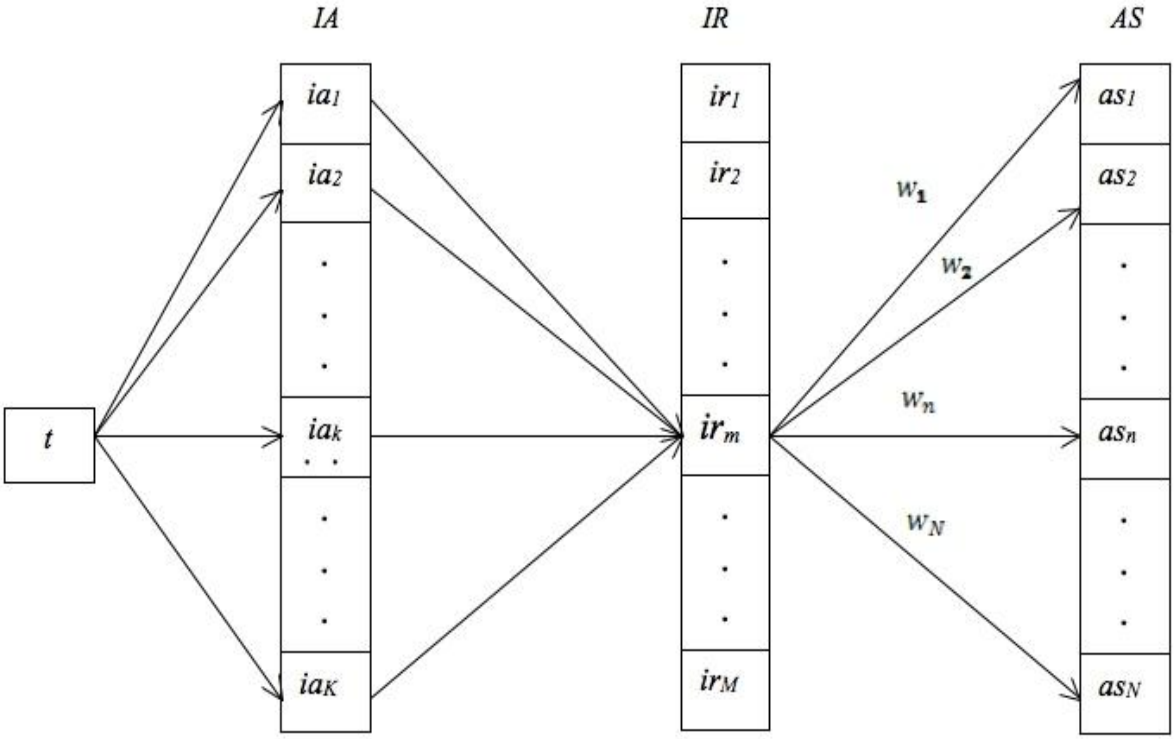

Рис. 1. Механизм формирования рисков, обусловленных реализацией угрозы t_i относительно информационного актива ia_m

В общем случае, принимая во внимание, что угроза может одновременно реализовываться через существующие уязвимости информационных активов ia_1, ia_2, ... ,ia_K, причем у каждого актива может быть несколько уязвимостей, вероятность реализации угрозы p_t определится формулой:

$$p_t(ir_m) = 1 - \prod_{k=1}^{K} (1 - p_t(ir_m / ia_k)), \qquad (13)$$

где каждая из условных вероятностей $p_t(ir_m / ia_k),\ k = \overline{1, K}$ рассчитывается в соответствии с формулой (12).

Потери организации, обусловленные действием угрозы t, определяются степенью подверженности отдельных активов организации изменению состояния информационного ресурса ir_m вследствие реализацией угрозы t, точнее, степенью и характером возникающих при этом искажений информации или компроментации ин-

формации, представленной данным ресурсом. Уровень потерь соответствует уменьшению общей стоимость этих активов (экономических, финансовых, имиджевых и т.п.), что зависит от свойств и особенностей информационных технологий, участвующих в создании данных активов или в обслуживании их функционирования. Чем выше уровень информатизации организации, тем в большей мере её активы зависят от реализации деструктивных влияний на информационные ресурсы организации.

Если стоимость актива $Q(as_n)$, $n=\overline{1,N}$, степень его подверженности влиянию информационной угрозы t – $w_n(t)$, величина потерь составляет $q(as_n/t)=w_n(t)Q(as_n)$. Общие потери, понесенные организацией в результате реализацией угрозы t относительно информационного ресурса ir_m, в этом случае определятся формулой:

$$Q(ir_m/t)=\sum_{n=1}^{N} w_n(t)Q(as_n). \qquad (14)$$

Значения $w_n(t)$, $n=\overline{1,N}$ задаются расчетным, чаще экспертным путем, иногда имеют вероятностный характер [6], представляя вероятность полной потери стоимости $Q(as_n)$ актива as_n в случае успешной реализации угрозы t относительно ресурса ir_m.

Зная значениями потерь (14) и их вероятностную характеристику (13), находим величину риска организации для случая реализации угрозы t, ориентированной на поражение информационного ресурса ir_m:

$$R_t(ir_m)=p_t(ir_m)Q(ir_m/t). \qquad (15)$$

Полученное частное решение следовало бы трансформировать для более общей постановки задачи, принимая во внимание практические особенности рисковых ситуаций в реальных организациях.

Во-первых, рисковые ситуации чаще всего создаются совместным действием ряда угроз $T=\{t_i\}$, $i=\overline{1,n}$, каждая из которых может осуществляться через определенную совокупность информационных активов IA, поражая некоторое множество информационных ресурсов IR, что в свою очередь приводит к изменению состояния активов IR и в конечном итоге определяет уровень обобщенных потерь (рис.2).

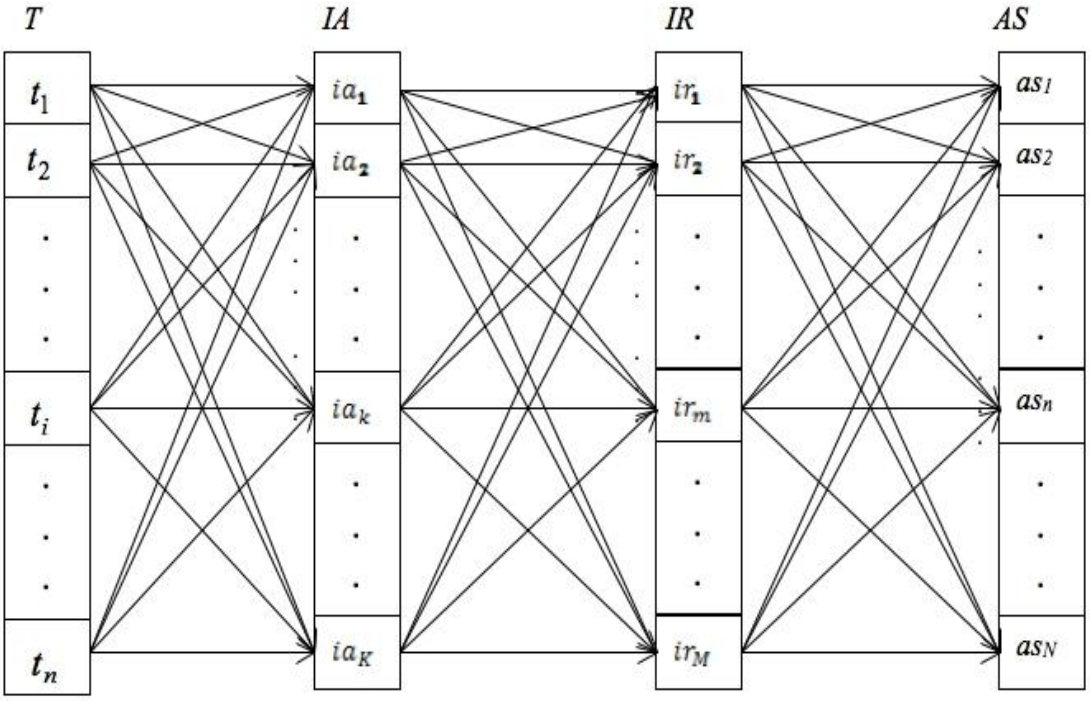

Рис. 2. Формирование потерь организации в условиях воздействия множества входных информационных угроз

Во-вторых, помимо громоздкости анализа собственно «траекторий» влияния множественных угроз на активы организации, возникает проблема учета их взаимовлияния, точнее, учета последствий совместных деструктивных воздействий разных угроз на одни и те же активы AS организации. Обычно принимаемая в этом случае гипотеза аддитивности последствий может привести к неоправданному завышению объема интегральных потерь, к абсурдному суммированию потерь взаимоисключающих последствий.

К сожалению, для множества угроз при больших объемах активов получить достаточно объективное заключение об уровне потерь путем поштучного рассмотрения воздействия каждой из угроз на активы организации сложно [7]. Приемлемый результат в создавшейся ситуации может быть получен путем сведения последствий реализации любой из угроз к анализу трех характеристик (состояний) информационных потоков, циркулирующих в организации: доступности, целостности и конфиденциальности информации, формирующей потоки. Для этого составляется схема информационных потоков организации. В точках «ввода» угроз (т.е. в уязвимых элементах информационных активов IA) выявляется характер влияния соответствующих угроз на состояние информации в проходящей через точку «ввода» части потоков, затем оцениваются результирующие характеристики потоков и их влияние на состояние активов организации, «подпитываемых» соответствующими потоками.

Эффективной мерой является также декомпозиция (фрагментирование) исходного множества активов IR на относительно независимые (функционально, организационно) подмножества [8], в пределах которых возможно практически автономное проведение АОР. В простейшем случае фрагментирование ресурсов IR влечет за собой разделение исходной совокупности активов AS на непересекающиеся подмножества характерной принадлежности: производственной, административной, управленческой и т.п., что существенно упрощает АОР.

Приоритезация информационных активов по степени их уязвимости. При проектировании и разработке систем защиты информации обычно оцениваются уровни деструктивного воздействия на объект риска актуальных информационных угроз с последующей их классификацией по интенсивности этого воздействия, что позволяет сконцентрировать усилия защиты на наиболее разрушительных угрозах. Однако, учитывая, что реализация этих угроз осуществляется через достаточно ограниченный набор уязвимостей ИС, при выборе комплекса защитных мероприятий крайне полезны и необходимы сведения о степени уязвимости эксплуатируемых информационных активов IA, например, значения интегральных рисков, происхождение которых связано с восприимчивостью этих активов к воздействию характерных угроз.

Представленная на рис. 3 схема иллюстрирует процедуру оценивания уязвимости информационного актива ia_k (сервер, рабочая станция, прикладная программа, администратор системы, авторизованный пользователь и т.п.) при его эксплуатации в ИС конкретной организации.

Сначала из предварительного анализа условий функционирования объекта риска (ИС) выявляется совокупность угроз t_1, t_2, t_i, t_n, представляющих опасность для актива ia_k. По схеме информационных потоков организации определяется набор информационных ресурсов ir_1, ir_2, ir_m, ir_M, на которые через актив ia_k распространяется деструктивное влияние четырех перечисленных выше угроз, и затем выявляются элементы активов AS, критичные к влиянию искажений, уничтожению или компрометации информационных ресурсов ir_1, ir_2, ir_m, ir_M.

Пусть $p_{ti}(ir_m / ia_k)$ – вероятность реализации одиночной угрозы t_i через уязвимость информационного актива ia_k с последующим поражением информационного ресурса ir_m. Степень подверженности актива as_n последствиям реализации угрозы t_i относительно информационного ресурса ir_m определим как $w_n(t_i, ir_m)$. Тогда значение риска потерь стоимости активов организации, зависящих от состояния ресурса ir_m, обусловленного уязвимостью информационного актива ia_k, составит

$$R(ir_m / t_i, ia_k) = p_{ti}(ir_m / ia_k)\sum_{n=1}^{N} w_n(t_i, ir_m)Q_n . \qquad (16)$$

Обобщение рисков $R(ir_m / t_i, ia_k)$ по всем информационным ресурсам, подверженным влиянию угрозы t_i, приводит к выражению:

$$R(ia_k / t_i) = \sum_{k=1,2,m,M} p_{ti}(ir_m / ia_k)\sum_{n=1}^{N} w_n(t_i, ir_m)Q_n . \qquad (17)$$

Степень подверженности актива as_n деструктивным последствиям реализации угрозы t_i определяется путем анализа схемы информационных потоков, поддерживающих те или иные информационные технологии, влияющие на стоимость активов организации, и оцениванием уменьшения стоимости актива, вызванной искажениями или компроментацией информационных ресурсов вследствие реализации угрозы t_i.

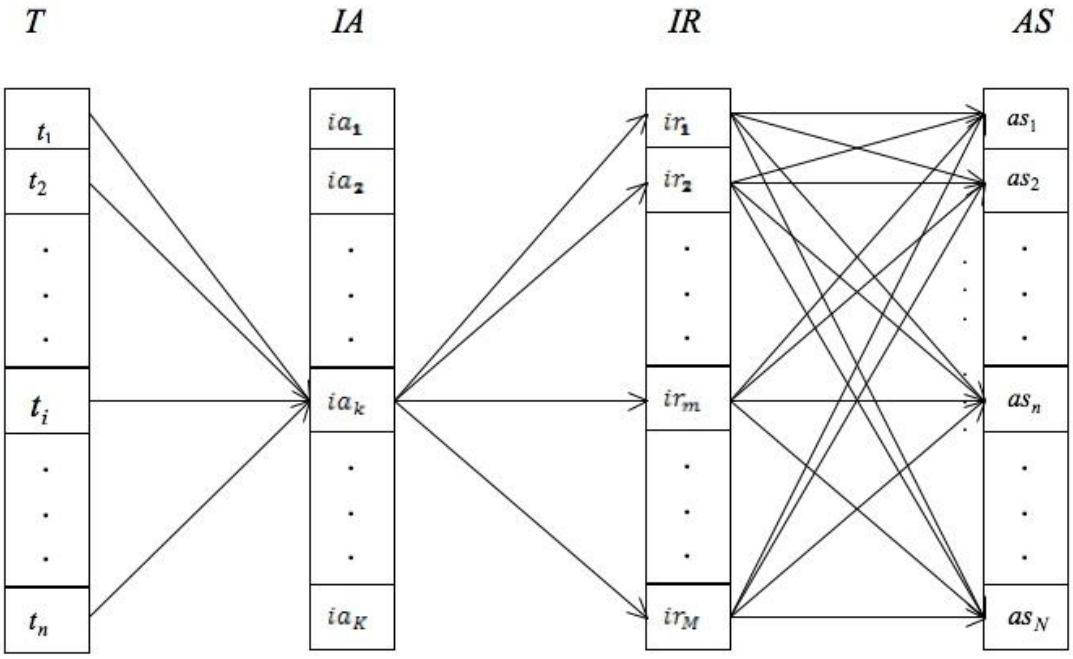

Рис. 3. Схема оценивания степени уязвимости информационного актива ia_k (сервер, рабочая станция, прикладная программа и т.п.) при его эксплуатации в составе ИС организации

Если предположить возможность выполнения раздельного анализа рисков реализаций каждой из угроз t_1, t_2, t_i, t_n и полагать справедливой гипотезу аддитивности последствий этих реализаций, то обобщенный риск организации, обусловленный уязвимостью информационного актива ia_k со стороны угроз t_1, t_2, t_i, t_n составит:

$$R(ia_k / t_1, t_2, t_i, t_n) = \sum_{l=1,2,i,n} [\sum_{k=1,2,m,M} p_{ti}(ir_m / ia_k) \sum_{n=1}^{N} w_n(t_i, ir_m) Q_n]. \quad (18)$$

Подобным образом можно оценить риски, обусловленные уязвимостями других информационных активов IA, и проранжировав эти риски, получить объективные сведения о степени приоритетности защиты тех или иных активов ИС. Очевидно, что в первую очередь защите подлежат информационные активы ИС, имеющие наивысшие уровни обобщенного риска (18) и, следовательно, наименее устойчивые к воздействию угроз (либо обладающие наибольшим деструктивным влиянием на зависимые от их состояния ресурсы и активы организации).

Выводы. В статье анализируются методологические аспекты вычисления обобщенного риска, обусловленного реализацией множественных атак и угроз в информационной системе. Рассмотрены механизмы формирования рисков, в частности, процессы развития деструктивных последствий реализации угроз и образования потерь. практические способы оценивания вероятностных параметров рисков и величин потерь, приоритезацию информационных активов информационной системы по степени их уязвимости.

ЛИТЕРАТУРА

[1]. Архипов А.Е. Применение среднего риска для оценивания эффективности защиты информационных систем. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. // науково-техн. зб. – Київ, 2007. – Вип.1(14). – с.60-67.

[2]. Архипов А.Е. Экспертно-аналитический подход к оцениванию информационных рисков. // Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту: Матеріали міжнародної наукової конференції (ISDMSI'2009). Том 1. – Херсон: ХНТУ, 2009. – 288с, с.246-249.

[3]. ДСТУ ISO/IEC TR13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій.

[4]. ISO / IEC 27005 – Information security risk management.

[5]. Архипов О.Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: моногр. / О.Є.Архипов, О.Є.Муратов. – К.: Наук.-вид. відділ НА СБ України, 2011. – 195с.

[6]. Архипов О.Є., Касперський І.П. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ-2007р, випуск 2(15). – С. 13-19.

[7]. Архипов О.Є. Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій //Захист інформації. – 2011. – №1(50), С. 42-47.
[8]. Архипов А.Е. Технология построения комбинированных измерительных шкал для оценивания значимости информации. // Сб. «Адаптивні системи автоматичного управління», Київ: Техніка, №13(33), 2008. – С. 153-158.

REFERENCES

[1]. Arkhypov A.E. (2007), «Application of average risk for assessment of effectiveness of information systems», Legal, regulatory and metrology systems of information security in Ukraine, Issue 1(14), pp.60 -67.
[2]. Arkhypov A.E. (2009), «Expert-analytical approach to the evaluation of information risks.», Intelligent Decision Support Systems and Problems of Computational Intelligence: Proceedings of the International Scientific Conference (ISDMSI'2009), Vol1., pp.246 - 249.
[3]. ISO/IEC TR 13335-3: 2003 – Information technology. Guidance on safety management of information technology. Part 3: Methods of information technology management protection.
[4]. ISO / IEC 27005 – Information security risk management.
[5]. Arkhypov A.E., Muratov A.E. (2011), «Criteria for possible damage to the national security of Ukraine in case of disclosure of information protected by the state», Monograph in scientific publications at department of National Academy of Security Service of Ukraine, p. 195.
[6]. Arkhypov A.E., Kaspersky I.P. (2007), «The methodology for predicting evaluation of damage caused by leakage of secret information.», Legal, regulatory and metrology systems of information security in Ukraine, Issue 2(15), pp.13 -19.
[7]. Arkhypov A.E. (2011), «Regarding methods of identification and evaluation systems assets of information technology», Information Security, Vol.1 (50), pp.42 -47.
[8]. Arkhypov A.E. (2008), «Technology for constructing combined measurement scales for evaluating the significance of the information.», Technology, Vol.13(33), pp.153 -158.

ПРАКТИЧНІ АСПЕКТИ ОЦІНЮВАННЯ РИЗИКІВ РЕАЛІЗАЦІЇ ЗАГРОЗ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Одна з нагальних проблем дослідження та експлуатації систем захисту інформації (СЗІ) – оцінювання узагальненого показника захищеності СЗІ, в якості якого часто виступає так званий інтегральний ризик. Це скалярний показник, що є відображенням набору часткових ризиків (ризиків атак, ризиків загроз, ризиків вразливостей окремих елементів інформаційних систем (ІС)). У статті сформульовані умови коректного відображення часткових ризиків в інтегральний. Розглянуто механізми виникнення ризиків, зокрема, процеси розвитку деструктивних наслідків реалізації загроз і утворення втрат. Досліджено проблеми, що виникають при оцінюванні імовірнісного параметра ризику і визначення рівня втрат у випадку множинних загроз. Запропоновано методику пріоритезации інформаційних активів ІВ за ступенем їх вразливості.
Ключові слова: ризик, інтегральний (узагальнений) ризик, сумарний ризик, ризик атак (загроз), механізм виникнення ризику, імовірнісний параметр ризику.

PRACTICAL ASPECTS OF RISK MANAGEMENT OF THREAT IN INFORMATION SYSTEM

One of the most urgent problems of research and exploitation of information security systems is the evaluation of the generalized index of protection information system, as which is often known as integral risk. This scalar measure is a reflection of a set of partial risks (risks of attacks, threats risk, vulnerability risk of individual elements of information systems (IS)). In the paper conditions of correct display of partial risks in integral is stated. Considered mechanisms of risk occurrence, processes of the destructive consequences of threats and formation of losses. The problems, which arising from the evaluation of probability parameters of risk and determine the level of losses in the case of multiple threats. The technique prioritize information assets IP according to their vulnerability.
Keywords: risk, integral risk, generalized risk, total risk, attacks, mechanism of risk occurrence, probability parameters of risk.

Архипов Александр Евгеньевич, доктор технических наук, профессор кафедры информационной безопасности Национального технического университета Украины «Киевский политехнический институт».
E-mail: sonet@zeos.net
Архипов Олександр Євгенійович, доктор технічних наук, професор кафедри інформаційної безпеки Національного технічного університету України «Київський політехнічний інститут».
Arkhypov Oleksandr, Dr. Sci. Tech., professor at the Department of Information Defense at National Technical University of Ukraine «Kyiv Polytechnic Institute».

Скиба Андрей Владимирович, аспирант Национального технического университета Украины «Киевский политехнический институт».
E-mail: andrewskyba@ukr.net
Скиба Андрій Володимирович, аспірант Національного технічного університету України «Київський політехнічний інститут».
Skyba Andrii, PhD graduate student National Technical University of Ukraine «Kyiv Polytechnic Institute».