УДК 004.056

С.И. Носков, А.А. Бутин, Л.Е. Соколова

Многокритериальная оценка уровня уязвимости объектов информатизации

Рассматривается формализованный способ оценки уязвимости объектов информатизации. Он предполагает построение агрегированного критерия уровня уязвимости в виде линейной свертки локальных критериев с применением методов теории принятия решений. При этом задача определения коэффициентов свертки сводится к поиску решения или квазирешения задачи линейного программирования. Предложен алгоритм оценки уровня компетентности привлекаемых экспертов.

Ключевые слова: информационная безопасность, уязвимость, линейное программирование, квазирешение, теория принятия решений, экспертная информация.

При создании инфраструктуры объектов информатизации (ОИ) на базе современных компьютерных систем и сетей неизбежно возникает вопрос их защищенности от различных угроз. Эти угрозы как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости, приводящие к нарушению безопасности информации на конкретном ОИ. Уязвимости неотделимы от ОИ и обусловливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и физического расположения.

Перечисленные обстоятельства диктуют настоятельную необходимость создания фундаментальной научной методологии комплексной оценки уровня безопасности ОИ. Представляется, что основой такой методологии могут и должны стать современные методы математического моделирования. Они являются признанным инструментом научного анализа сложных, с множеством внутренних и внешних взаимосвязей объектов различной природы, поскольку позволяют на модельном уровне формализовывать закономерности, присущие этим объектам, посредством разработки их качественных абстрактных образов. Это открывает широкие возможности в повышении эффективности вырабатываемых управляющих воздействий, поскольку при этом экспериментирование может проводиться не с «живой» системой, а с её математической моделью.

Этапом, предваряющим собственно настроение математической модели любого объекта, является выбор показателей (факторов, переменных), определяющих его функционирование. К сожалению, к настоящему времени как в научных, так и в нормативных изданиях не описан (не определен, не задан, не формализован) какой-либо один показатель (фактор), в полной мере отражающий уровень (степень, меру) уязвимости ОИ. Вместе с тем известны частные характеристики ОИ, «отвечающие» за те или иные локальные стороны в оценке такой комплексной уязвимости. Так, например, в работе [1] для удобства анализа отдельные уязвимости разделены на классы (они обозначаются заглавными буквами), которые, в свою очередь, распадаются на группы (обозначаются римскими цифрами), а последние – на подгруппы (обозначаются строчными буквами). Определено три класса: [A] объективные, [B] субъективные и [C] случайные уязвимости.

При этом объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-физическими методами парирования угроз безопасности информации.

К ним можно отнести:

[A.I] сопутствующие техническим средствам излучения:

- [A.I.a] электромагнитные (побочные излучения элементов и кабельных линий технических средств (ТС), излучения на частотах работы генераторов, на частотах самовозбуждения усилителей);
- [A.I.b] электрические (наводки электромагнитных излучений на линии и проводники, просачивание сигналов в цепи электропитания, в цепи заземления, неравномерность потребления тока электропитания);

• [A.I.c] звуковые (акустические, виброакустические);

[A.II] активизируемые:

• [A.II.a] аппаратные закладки (устанавливаемые в телефонные линии, в сети электропитания, в помещениях, в ТС);

• [A.II.b] программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии программного обеспечения (ПО));

[A.III] определяемые особенностями элементов:

• [A.III.a] элементы, обладающие электроакустическими преобразованиями (телефонные аппараты, громкоговорители и микрофоны, катушки индуктивности, дроссели, трансформаторы и пр.);

• [A.III.b] элементы, подверженные воздействию электромагнитного поля (магнитные носители, микросхемы, нелинейные элементы, подверженные высокочастотному навязыванию);

[A.IV] определяемые особенностями защищаемого объекта:

• [A.IV.a] местоположением объекта (отсутствие контролируемой зоны, наличие прямой видимости объектов, удаленных и мобильных элементов объекта, вибрирующих отражающих поверхностей);

• [A.IV.b] организацией каналов обмена информацией (использование радиоканалов, глобальных открытых информационных сетей, арендуемых каналов).

Субъективные уязвимости зависят от действий сотрудников и в основном устраняются организационными методами и программно-аппаратными средствами:

[B.I] ошибки:

• [B.I.a] при подготовке и использовании ПО (в том числе при разработке алгоритмов и ПО, его инсталляции, загрузке, эксплуатации, вводе данных);

• [B.I.b] при управлении сложными системами (при использовании возможностей самообучения систем, настройке сервисов универсальных систем, организации управления потоками информации);

• [B.I.c] при эксплуатации ТС (при включении/выключении ТС, использовании средств охраны и средств обмена информацией);

[B.II] нарушения:

• [B.II.a] режима охраны и защиты (доступа на объект и к ТС);

• [B.II.b] режима эксплуатации ТС (энергообеспечения, жизнеобеспечения);

• [B.II.c] режима использования информации (обработки и обмена информацией, хранения и уничтожения носителей, уничтожения производственных отходов и брака);

• [B.II.d] режима конфиденциальности (уволенными, а также сотрудниками в нерабочее время).

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, малопредсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности. К ним можно отнести:

[C.I] сбои и отказы:

• [C.I.a] отказы и неисправности ТС (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, охрану и контроль доступа);

• [C.I.b] старение и размагничивание носителей информации (дискет, съемных носителей, жестких дисков, элементов микросхем, кабелей и соединительных линий);

• [C.I.c] сбои ПО (операционных систем и СУБД, прикладных, сервисных и антивирусных программ);

• [C.I.d] сбои электроснабжения (оборудования, обрабатывающего информацию, обеспечивающего и вспомогательного оборудования);

[C.II] повреждения:

• [C.II.a] жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации, кондиционирования и вентиляции);

• [C.II.b] ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий, корпусов технологического оборудования).

В рамках теории принятия решений разработан целый спектр методов, позволяющих объединять частные характеристики (критерии, показатели уязвимостей) объектов различной природы в некие ненаблюдаемые в реальности агрегаты (свертки), что позволяет оценивать обобщенные свойства объектов (в нашем случае уязвимость (ОИ) (см., например, [2–6]). Будем основывать дальнейшее изложение в основном на работах [5, 6], в которых представлена методика объединения локальных критериев в обобщенные агрегаты с использованием аппарата линейного программирования.

Итак, пусть в распоряжении исследования есть численная информация о g критериях уязвимости r элементов отдельного объекта информатизации, т.е. матрица $\mathbf{X}=\left\|x_{ij}\right\|,i=\overline{1,r},j=\overline{1,g}$.

Пусть к оценке уязвимости каждого элемента ОИ привлечены p экспертов. На основе использования их сравнительных высказываний и матрицы **X** необходимо построить линейную свертку частных критериев (агрегированный критерий) вида

$$R=\sum_{j=1}^{g}\alpha_j x_j, \tag{1}$$

где j – номер частного критерия.

Далее организуется процедура независимого опроса экспертов относительно сравнительной уязвимости пар ОИ. При этом каждый эксперт производит свою оценку только по отношению к парам, уязвимость ОИ в которых он может с уверенностью сравнить.

Каждый i-й эксперт строит индексное множество $M^i=\left\{(a_1^i,b_1^i),(a_2^i,b_2^i),...,(a_{l_i}^i,b_{l_i}^i)\right.$ пар объектов, в которых первый объект более (не менее) уязвим, чем второй, и множество $N^i=\left\{(c_1^i,d_1^i),(c_2^i,d_2^i),...,(c_{s_i}^i,d_{s_i}^i)\right\}$ пар объектов, уязвимость которых, по мнению эксперта, «примерно» одинакова, $i=\overline{1,p}$.

Здесь l_i и S_i – размерность множеств M_i и N_i соответственно. При этом не исключаются ситуации, когда какое-то из множеств N_i или M_i оказывается пустым, поскольку эксперт может затрудниться в указании требуемых пар.

В случае непротиворечивости экспертных высказываний должны быть совместны системы линейных равенств и неравенств

$$R(C_j^i)=R\left(d_j^i\right),i=\overline{1,p},j=\overline{1,l_i} \tag{2}$$

$$R(a_j^i)\geq R\left(b_j^i\right),i=\overline{1,p},j=\overline{1,S_i} \tag{3}$$

где через $R(k)$ обозначена уязвимость k-го объекта, $k=\overline{1,r}$.

Сделаем одну необходимую оговорку. А именно, чем больше значение $R(k)$, тем выше уязвимость k-го элемента объекта. Значит, для достижения однородности обобщенного и частных критериев необходимо полагать, что каждый фактор x_j позитивно влияет на уязвимость, т.е. усиливает (увеличивает) ее. А в приведенном выше перечне частных характеристик уязвимости ОИ есть такие, которые уязвимость снижают. Такие характеристики x_i необходимо преобразовывать, например, посредством использования переменных $1/x_i$. Поэтому в (1) естествен переход от переменных x_i к переменным $\tilde{x}_i$, задаваемым по правилу:

$\tilde{x}_i=x_i$, если i-й фактор увеличивает уязвимость объекта, и

$\tilde{x}_i=1/x_i$ в противном случае. Обозначим это правило цифрой (4).

Таким образом, свертка (1) заменится на следующую:

$$\tilde{R}=\sum_{j=1}^{g}\tilde{\alpha}_j\tilde{x}_j\ , \tag{5}$$

где, в соответствии с (4), $\tilde{x}_i\geq 0,j=\overline{1,g}$. Для агрегированного показателя уязвимости $\tilde{R}$ очевидным образом остаются справедливыми системы равенств (2) и неравенств (3).

Введем в рассмотрение переменные y_{ej}^{1i} и y_{ej}^{2i} следующим образом:

$$y_{ej}^{1i}=x_{a_e^i j}-x_{b_e^i j},(a_e^i,b_e^i)\in M^i,i=\overline{1,p},j=\overline{1,g},$$

$$y_{ej}^{2i}=x_{c_e^i j}-x_{d_e^i j},(c_e^i,d_e^i)\in N^i,i=\overline{1,p},j=\overline{1,g}.$$

Тогда равенства (2) и неравенства (3) примут соответственно вид

$$\sum_{j=1}^{g}\tilde{\alpha}_j y_{ej}^{1i}\geq 0,e=\overline{1,l_i},i=\overline{1,p}\ , \tag{6}$$

$$\sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{2i} = 0, e = \overline{1, l_i}, i = \overline{1, p}. \quad (7)$$

В соответствии с приемом, принятым в теории принятия решений, потребуем, чтобы так называемая разрешающая способность системы неравенств (6) была как можно выше. Формально это требование представимо в форме

$$\sum_{i=1}^{p} \beta_i \sum_{e=1}^{l_i} \sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{1i} \to \max. \quad (8)$$

Здесь β_i – уровень компетентности *i*-го эксперта, при этом $\beta_i > 0, i = \overline{1, p}, \sum_{i=1}^{p} \beta_i = 1$.

При отсутствии информации об оценках уровня компетентности экспертов будем полагать $\beta_i = 1$ для всех $i = \overline{1, p}$.

Учтем еще несколько важных соображений. Для обеспечения возможности сравнения степени уязвимости разных по характеру и масштабу элементов ОИ агрегированному показателю уязвимости $\tilde{R}$ необходимо придать относительный характер. Это можно делать, например, следующим образом.

Рассчитаем максимальные значения преобразованных значений частных критериев уязвимости: $\tilde{x}_j^+ = \max\limits_{j=1,g} \tilde{x}_j$.

Потребуем, чтобы уязвимость некоего объекта с максимальными значениями ее частных характеристик составляла 100%:

$$\sum_{j=1}^{p} \tilde{\alpha}_j \tilde{x}_j^+ = 100. \quad (9)$$

Требование строгой положительности параметров $\tilde{\alpha}_j$, а также то обстоятельство, что каждый частный показатель уязвимости обязательно должен обладать какой-то по крайне мере минимальной значимостью, можно формализовать следующим образом:

$$\tilde{\alpha}_j \tilde{x}_j^+ \geq \gamma_j, j = \overline{1, g}. \quad (10)$$

В качестве заданных заранее положительных чисел γ_j можно использовать, например, такие: $\gamma_j = \frac{10}{g}$, поскольку, если принять равными вклады каждой частной характеристики уязвимости в их агрегат, значения таких вкладов будут равны величине $\frac{100\%}{g}$.

Таким образом, задача построения агрегированного критерия уязвимости ОИ $\tilde{R}$ сводится к задаче линейного программирования (ЛП) с ограничениями (6), (7), (9), (10) и целевой функцией (8).

В том случае, если изначально уровень компетентности экспертов неизвестен ($\beta_i = \frac{1}{p}$ для всех *i*), то после решения указанной задачи ЛП этот уровень можно вычислить, рассчитав среднюю разрешающую способность высказываний каждого эксперта:

$$\beta_i = \sum_{e=1}^{l_i} \sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{1i} \Bigg/ \sum_{h=1}^{p} \sum_{e=1}^{l_h} \sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{1h}, \quad (11)$$

т.е. чем выше суммарная разрешающая способность ограничений (6), тем выше уровень компетентности соответствующего эксперта.

Разумеется, такой способ оценивания уровня компетентности экспертов является в определенной мере относительно условным, поскольку жестко привязан к виду функции, задающей свертку критериев. Если, в частности, вместо линейной функции (1) использовать более гибкую, например полином, результаты могут оказаться иными.

Предположим теперь, что задача ЛП (6)–(10), несовместна, т.е. экспертные высказывания взаимно противоречивы. В этом случае в соответствии с теорией решения некорректных задач

А.Н. Тихонова нужно искать квазирешение указанной задачи, использовав при этом прием, описанный в [4].

Введем в рассмотрение новые неотрицательные переменные u_e^i, v_e^i, t_e^i и преобразуем ограничения (6) и (7) к виду

$$\sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{1i} + t_e^i \geq 0, e = \overline{1, l_i}, i = \overline{1, p}, \quad (12)$$

$$\sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{2i} + u_e^i - v_e^i = 0, e = \overline{1, l_i}, i = \overline{1, p}. \quad (13)$$

Введенные переменные представляют собой искажения, внесенные в ограничения (6) и (7), гарантирующие их совместность. Эти искажения необходимо минимизировать, заменив функционал (8) на

$$\sum_{i=1}^{p} \sum_{e=1}^{l_i} (t_e^i + u_e^i + v_e^i) \to \min. \quad (14)$$

Сформированная таким образом задача ЛП (9), (10), (12)–(14) также будет позволять рассчитывать коэффициенты линейной свертки (5).

Далее, при оценивании уровня компетентности каждого эксперта в этом случае следует исходить из соображения – чем меньше суммарное искажение ограничений, следующих из его экспертных высказываний, тем этот уровень выше, т.е. $\beta_i = 1 - \sum_{e=1}^{l_i} (t_e^i + u_e^i + v_e^i) \Big/ \sum_{i=1}^{p} \sum_{e=1}^{l_i} (t_e^i + u_e^i + v_e^i)$.

Для того чтобы обеспечить равенство единице суммарных уровней компетенции, полученные значения β_i необходимо соответствующим образом пронормировать.

Для оценки уровня компетентности экспертов, высказывания которых непротиворечивы, следует воспользоваться описанным выше приемом.

В следующей своей публикации авторы намерены описать практическое использование предложенной в работе методики для оценки уязвимости конкретных ОИ.

Литература

1. Классификация угроз информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml, свободный (дата обращения: 11.04.2014).

2. Носков С.И. Управление системой обеспечения пожарной безопасности на региональном уровне / С.И. Носков, В.П. Удилов. – Иркутск: ВСИ МВД России, 2003. – 151 с.

3. Носков С.И. Газификация сельской местности: целевое программирование пожарной безопасности / С.И. Носков, В.Г. Подушко, В.П. Удилов. – Иркутск: ИрГТУ, 2001. – 150 с.

4. Носков С.И. Критериальная оценка обстановки с пожарами АТЕ Сибири и Дальнего Востока / С.И. Носков, В.П. Удилов, О.В. Бутырин // Проблемы деятельности правоохранительных органов и противопожарных служб: матер. II межвуз. науч.-практ. конф. – Иркутск: ИВШ МВД России, 1996. – С. 109–111.

5. Носков С.И. Технология моделирования объектов с нестабильным функционированием и неопределенностью в данных. – Иркутск: Облинформпечать, 1996. – 320 с.

6. Носков С.И. Оценка уровня уязвимости объектов транспортной инфраструктуры: формализованный подход / С.И. Носков, В.А. Протопопов // Современные технологии. Системный анализ. Моделирование. – 2011. – № 4. – С. 241–244.

Носков Сергей Иванович
Д-р техн. наук, профессор, профессор каф. информационных систем и защиты информации
Иркутского государственного университета путей сообщения (ИрГУПС)
Тел.: 8-914-902-24-94
Эл. почта: noskov_s@irgups.ru

Бутин Александр Алексеевич
Канд. физ.-мат. наук, доцент, доцент каф. информационных систем и защиты информации ИрГУПС
Тел.: 8-908-662-57-05
Эл. почта: butin_aa@mail.ru

Соколова Людмила Евгеньевна
Ассистент каф. информационных систем и защиты информации ИрГУПС
Тел.: 8-904-120-81-84
Эл. почта: LESokol1987@yandex.ru

Noskov S.I., Butin A.A., Sokolova L.E.
Multicriterial assessment of the level of vulnerability of the objects of informatization

The article considers a formalized way of assessing the vulnerability informatization objects. Itinvolves the construction of aggregated criterion of the level of vulnerability in the form of a linear convolution of local criteria with the use of methods of the theory of decision-making. The problem of determining the coefficients of the convolution is reduced to finding a solution or quasidecision of linear programming problems. An algorithm for evaluation of the level of competence of experts.
Keywords: information security, vulnerability, linear programming, quasidecision, theory of decision-making, expert information.