УДК 004

Комплексный подход к оценке угроз безопасности информации с оценкой состояния объекта защиты при нарушении безопасности

В статье рассмотрены проблемные вопросы оценки эффективности обеспечения защиты информации. Авторы продолжили разработку методологии организации защиты информации, проблематика которой была поднята на страницах журнала. Предложено описывать комплексный подход к оценке угроз безопасности информации, оценивая состояние объекта защиты при нарушении безопасности с помощью частного интегрального показателя защищенности, характеризующего возможности по нанесению ущерба при ее реализации, по которому производится ранжирование.

Ключевые слова:
информационная безопасность, защита информации, угроза безопасности.

Авторами статьи на страницах предыдущего номера журнала [1] был разработан и предложен методический подход к оценке вероятностей реализации угроз безопасности информации (УБИ). Как было указано, проблематика исследований в данной предметной области связана со сложностью оценки эффективности обеспечения безопасности информации. Это обусловлено неопределенностью режимов и характера эксплуатации объектов информационных технологий (ОИТ) и средств защиты информации (СЗИ) по причине отсутствия полной информации обо всех режимах их функционирования, а также появлением различных видов угроз, бурным развитием современных технических средств воздействия на информационные ресурсы потенциальным нарушителем и возможностью появления новых способов и средств нарушения информации (новых угроз) [1].

Ю.Е. КУЛЕШОВ,
канд. воен. наук, доцент,
начальник военного факультета

А.А. БОГАТЫРЕВ,
канд. воен. наук,
зам. начальника военного факультета
по учебной и научной работе

С.И. ПАСКРОБКА,
канд. воен. наук, доцент,
начальник кафедры ТиОП военного факультета

УО «Белорусский государственный университет информатики и радиоэлектроники»

С.Н. КАСАНИН
канд. техн. наук, доцент,
заместитель директора по науке ГП «НИИ ТЗИ»

Рассуждая и вырабатывая концептуальные подходы к комплексной оценке УБИ, отметим следующее.

На наш взгляд, для построения комплексной защиты информации необходимо выявить в первую очередь УБИ и оценить их последствия, а именно опасность каждой угрозы. Предлагается формирование методологии выявления УБИ осуществлять по следующим направлениям:

– систематизация и статистическая оценка атак и попыток несанкционированного доступа к объектам информации;

– экспериментальное тестирование информационных систем (ИС) на предмет обнаружения уязвимых мест, использование которых возможно для реализации угроз;

– создание аналитических и имитационных моделей процессов функционирования ИС, угроз безопасности и генераторов атак;

– экспертный анализ и экспертные оценки с привлечением специалистов – системных администраторов, администраторов безопасности, аудиторов ИБ и других специалистов в области безопасности информации.

Следует отметить, что оценка УБИ является одним из основных этапов процесса анализа и управления рисками при создании и эксплуатации ИС. Она должна включать априорную оценку на этапе разработки, уточненную периодическую оценку в процессе эксплуатации с учетом информации мониторинга, выявления нарушений информационной безопасности (ИБ) и динамического управления рисками. В этом случае оценку следует проводить с использованием моделей общей оценки угроз, которые являются основой оценки как самих УБИ, так и потерь, которые могут иметь место при их проявлении. Модели данного типа важны еще и тем, что именно на них в основном выявлены те условия, при которых такие оценки могут быть адекватны реальным процессам защиты информации. К настоящему времени разработаны различные табличные, диаграммные, формализованные, имитационные модели УБИ. Следует отметить, что, несмотря на достоинства этих моделей, ни одна из них не позволяет одновременно учесть три основных параметра – уязвимость, активизируемую атакой, метод ее реализации и возможные последствия. Другими словами, возникает противоречие между теорией и практикой информационной защиты из-за неразрешенности вопросов в подходах к комплексности оценки УБИ.

Предлагаемый авторами статьи порядок комплексной оценки и ранжирования УБИ приведен на рис. 1.

Для определения потенциала УБИ в этом случае целесообразно использовать частный интегральный показатель защищенности:

$$R_{cpi} = \sum_k \sum_j r_{ikj} P_i = \sum_i r_{ij} P_i, \quad j = \overline{1, J}. \tag{1}$$

Он отражает средний риск нанесения ущерба при реализации угрозы определенного вида и характеризует степень ее опасности. В зависимости от априорного описания оценки показатель может быть в т. ч. нечетким статистическим и нечетким.

В первом случае для определения элементов множества рисков используются вероятностные оценки нечеткого случайного события:

$$\text{вероятность } p\left(r_{ikj}\right) = \int_{-\infty}^{\infty} f\left(r_{ikj}\right) \mu\left(r_{ikj}\right) dr_{ikj}; \tag{2}$$

математическое ожидание

$$Er_{ikj} = \left(E\underline{r}_{ikj}(\mu), E\bar{r}_{ikj}(\mu)\right); \tag{3}$$

дисперсия

$$Dr_{ikj} = 0{,}5 \int_0^1 \left[\left(\underline{r}_{ikj}(\mu) - E\underline{r}_{ikj}(\mu)\right)^2 + \left(\bar{r}_{ikj}(\mu) - E\bar{r}_{ikj}(\mu)\right)^2 \right] d\mu, \tag{4}$$

где $\underline{r}, \bar{r}$ – соответствующие ветви функции принадлежности при обратном отображении $\mu = \left(\underline{\mu}, \bar{\mu}\right), 0 \le \mu \le 1$.

Для определения потенциала атаки используются формулы теории вероятностей, поскольку в данном случае, кроме нечеткости по Заде, применяются дополнительные операции, такие как включение, алгебраическая сумма и алгебраическое произведение по Бандлеру и Кохоуту, эквивалентность.

При втором подходе для определения потенциала атаки операция суммирования определяется выражением

$$\sum_\xi r_\xi = \left\{ \sum_\xi r_\xi; \sum_\xi \mu\left(\sum_\xi r_\xi \right) \right\}, \tag{5}$$

в котором суммирование элементов носителей является скалярным, а значение функции принадлежности вычисляется согласно правилу центра тяжести, используемому в операции дефаззификации:

$$\sum_\xi \mu\left(\sum_\xi r_\xi \right) = \frac{\sum_\xi r_\xi \mu\left(r_\xi\right)}{\sum_\xi r_\xi}. \tag{6}$$

Таким образом, предложенный комплексный подход к оценке и ранжированию УБИ предусматривает использование частного интегрального показателя защищенности, характеризующего возможности по нанесению ущерба при ее реализации, по которому и производится ранжирование.

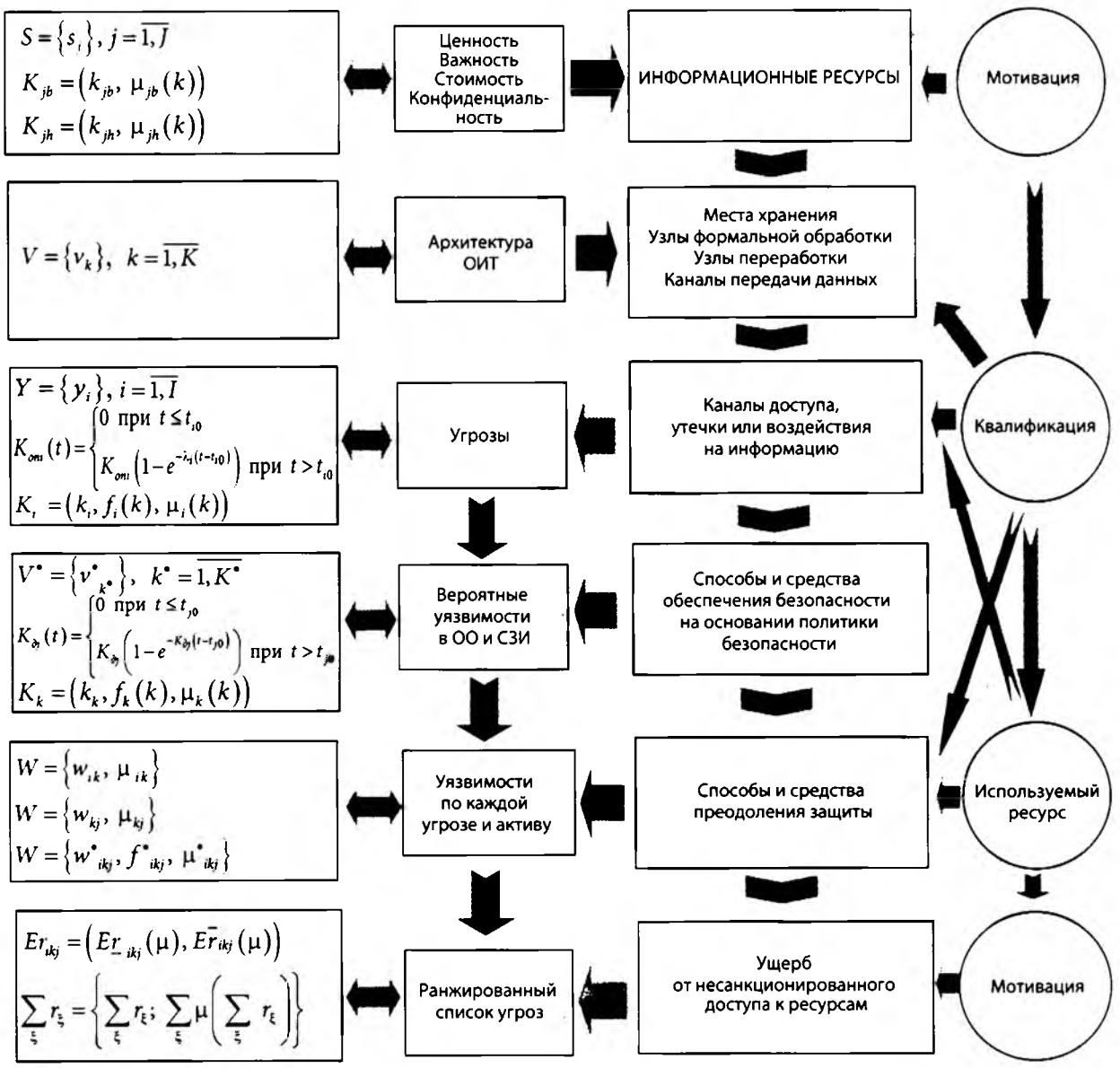

Рисунок 1 – Порядок оценки и ранжирования угроз безопасности

Рассуждая далее, выработаем подход к оценке состояний объекта оценки (ОО) при нарушении безопасности.

Итак, внешняя среда характеризуется нечетким множеством угроз активам

$$Y=\{y_i, \mu(y_i)\}, i=\overline{1,I}, \quad (7)$$

элементы которого определяются нечетким случайным коэффициентом опасности в качестве его динамической характеристики. В общем случае данный коэффициент можно описать выражением

$$x_i(t)=\begin{cases}0 \text{ при } t\le t_{i0}\\ K_i\left(1-e^{-\lambda_i(t-t_{i0})}\right) \text{ при } t>t_{i0},\end{cases} \quad (8)$$

где $K_i=\prod_{\xi_1=1}^{\Xi_1} k_{i\xi_1}$, $\lambda_i=\prod_{\xi_2=1}^{\Xi_2}\lambda_{i\xi_2}$,

t_{i0} – параметры угрозы.

ОО характеризуется двумя множествами: уязвимостей

$$V=\{v_k\}, k=\overline{1,K} \quad (9)$$

и активов (информации или ресурсов)

$$A=\{a_j\}, j=\overline{1,J}. \quad (10)$$

Уязвимости предлагается характеризовать коэффициентом доступности, который является их динамической характеристикой и в общем случае определяется выражением

$$v_k(t)=\begin{cases}0 \text{ при } t\le t_{k0}\\ K_k\left(1-e^{-K_k(t-t_{k0})}\right) \text{ при } t>t_{k0},\end{cases} \quad (11)$$

где $K_{ij}=\prod_{\varsigma=1}^{\Sigma_1}K_{j\varsigma}$, t_{ij0} – параметры уязвимости.

Коэффициенты K_j, K_k являются нечеткими случайными величинами:

$$K_i=\left(k_i, f_i(k), \mu_i(k)\right), K_k=\left(k_k, f_k(k), \mu_k(k)\right), \quad (12)$$

где k_η – оценочное значение соответствующего коэффициента (среднее значение),
$f_\eta(k)$, $\mu_\eta(k)$ – случайная и нечеткая составляющие нечеткой случайной величины.

Активы характеризуются нечетким коэффициентом ценности $K_{jh}=\left(k_{jh}, \mu_{jh}(k)\right)$ со стороны нарушителей (важность, ценность и степень заинтересованности в их получении) и коэффициентом ценности $K_{jb}=\left(k_{jb}, \mu_{jb}(k)\right)$ со стороны их владельцев (важность, стоимость, влияние на организацию, возможность восстановления и др.).

Между угрозами безопасности и уязвимостями ОО существует однозначная связь, образующая 2-дольный H-вершинный граф:

$$G=(Y, V, E_H), \quad (13)$$

где $E_H=\{e_h\}=\{e_{ij}\}, h=\overline{1,H}, H<I\times J$ – множество ребер графа G;
$e_h=(y_i, v_k)=\{0,1\}$.

Ребро $e_h=1$, если угроза y_i может быть реализована через уязвимость v_k, т. е.

$$\left(\exists y_i\in Y\right)\left(\exists v_k\in V\right)\ \left(\exists e_{ik}\right)\left(e_{ik}=1\right). \quad (14)$$

Каждому ребру $e_{ik}=(y_i, v_k)$ приписан вес w_{ik}, являющийся элементом нечеткого множества

$$W=\{w_{ik}, f_{ik}, \mu_{ik}\}, \quad (15)$$

где $w_{ik}=k_{ik}$, – элемент-носитель, означающий коэффициент опасности определенной угрозы при ее реализации через определенную уязвимость;
f_{ik}, μ_{ik} – совместные плотность распределения и функция принадлежности соответственно.

Уязвимости и активы также образуют 2-дольный D-вершинный граф:

$$G=(V, A, E_d), \quad (16)$$

где $E_d=\{e_d\}=\{e_{kj}\}, d=\overline{1,D}, D<K\times J$ – множество ребер графа G;
$e_d=(v_k, a_j), e_d=\{0,1\}$ – ребро графа G, удовлетворяющее условию
$\left(\exists v_k\in V\right)\left(\exists a_j\in A\right)\ \left(\exists_{kj}\right)\left(e_{kj}=1\right)$.

Каждому ребру $e_{kj}=(v_k, a_j)$ приписан вес w_{kj}, являющийся элементом нечеткого множества

$$W=\{w_{kj}, \mu_{kj}\}, \quad (17)$$

где $w_{kj}=k_{kj}$ – коэффициент опасности данной уязвимости для данного актива;
μ_{kj} – совместная функция принадлежности.

Объединение графов $G=(Y, V, E_H)$ и $G=(V, A, E_D)$ приводит к 3-дольному $L=H\times D$-вершинному графу

$$G=(Y, V, A, E_L). \quad (18)$$

Результирующее открытое ребро $e_{ikj}=\left(y_i, v_k, a_j\right)=\{0, 1\}$ множества ребер $E_L=\{e_l\}=\{e_{ikj}\}$, $l=\overline{1,L}$ графа G удовлетворяет условию

$$\left(\exists y_i\in Y\right)\left(\exists v_k\in V\right)\left(\exists a_j\in A\right)\ \left(\exists e_{ikj}\right)\left(e_{ikj}=1\right). \quad (19)$$

Каждому ребру $e_{ikj}=(y_i, v_k, a_j)$ приписан вес w_{ikj}, являющийся элементом случайного нечеткого множества

$$W=\{w_{ikj}, f_{ikj}, \mu_{ikj}\}, \quad (20)$$

где $w_{ikj}=k_{ikj}$ – коэффициент возможности принятия ОО состояния нарушения ИБ (ikj), характеризующий возможность реализации угрозы через определенную уязвимость на определенный актив;
μ_{ikj} – функция принадлежности элемента $w_{ikj}=k_{ikj}$ нечеткому множеству $W=\{w_{ikj}, \mu_{ikj}\}$.

Граф $G=(Y, V, A, E_L\}$ представляет собой граф состояний ОИТ с позиций ИБ (рис. 2). Он характеризует множество состояний ОО $\Theta=\{\theta_{ikj}\}$ при нарушении ИБ с учетом заинтересованности нарушителя, характеризуемой коэффициентом ценности активов $K_{ih}=(k_{ih}, \mu_{ih}(k))$.

Для определения взаимосвязи между элементами множеств $Y=\{y_i\}$, $i=\overline{1,I}$, $V=\{v_k\}$, $k=\overline{1,K}$ и $A=\{a_j\}$, $j=\overline{1,J}$ можно использовать базовые положения о сотрудничестве, конфликте и безразличии между подсистемами $\Im_1$ и $\Im_2$, входящими в окружение некоторой системы $\Im=\{\Im_1, \Im_2, \ldots, \Im_n\}$, суть которых заключается в следующем:

если $q\left(\Im_i, \Im_j\right)<q\left(\Im_i, \overline{\Im_j}\right)$, то
$\Im_j \Re\left(\overline{\Im_j}\right)\Im_j$, конфликт между $\Im_j$ и $\Im_i$,

если $q\left(\Im_i, \Im_j\right)>q\left(\Im_i, \overline{\Im_j}\right)$, то (21)
$\Im_j \overline{\Re}_c\left(\overline{\Im_j}\right)\Im_i$, сотрудничество между $\Im_j$ и $\Im_i$,

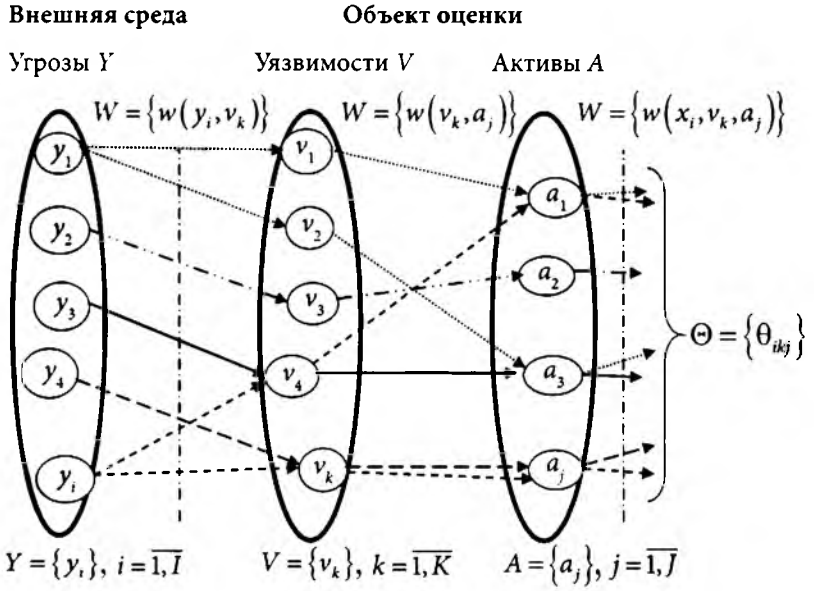

Рисунок 2 – Граф состояний объекта оценки

если $q(\Im_i,\Im_j)=q(\Im_i,\overline{\Im}_j)$, то

$\Im_i \Re_6(\Im_j)\Im_i$, безразличие между $\Im_j$ и $\Im_i$,

где q – функция полезности системы; $\overline{\Im}_j=\varnothing$. Мера структурного взаимодействия при $\Im_j=2$ определяется соотношением

$$\mu_{ij}(\overline{\Im}_j)=q(\Im_i,\Im_j)-q(\Im_i,\overline{\Im}_j)=\frac{\partial q(\Im_i,\overline{\Im}_j)}{2\partial\Im_j}\Im_j. \quad (22)$$

Таким образом, отсутствие механизмов достоверного подтверждения качества и достаточности средств защиты и недостаточная проработка вопросов моделей системы защиты, системы показателей и критериев безопасности ИТ обусловливают необходимость развития нормативно-методической базы, методик и моделей оценки защищенности на основе системного подхода. Первостепенным направлением можно назвать разработку моделей систем безопасности, критериев и показателей защищенности, методов их оценки и оценки элементов безопасности, методик оценки защищенности на всех этапах жизненного цикла ИТ. Также важна динамическая оценка рисков на основе системного подхода. В данном случае первостепенное значение имеют только те свойства элементов защиты, которые определяют взаимодействие друг с другом, оказывают влияние на систему в целом и на достижение поставленной цели.

ЛИТЕРАТУРА

1. **Кулешов, Ю.Е., Паскробка, С.И., Сергиенко, В.А., Касанин, С.Н.** Методический подход к оценке вероятностей реализации угроз безопасности информации / Ю.Е. Кулешов, С.И. Паскробка, В.А. Сергиенко, С.Н. Касанин // Научно-производственный журнал «Веснік сувязі». – 2017. – № 5. – С. 56–59.
2. **Шариков, П.А.** США хотят быть планетарным модератором. Американская глобальная стратегия развития киберпространства в полицентричном мире / П.А Шариков // Зарубежное военное обозрение. – 2011. – № 2. – С. 54–59.
3. **Казаковцев, А.В.** НАТО и кибербезопасность / А.В. Казаковцев // Вестник Волгоградского государственного университета – 2012. – № 2. – С. 109–114.
4. **Безкоровайный, М.М.** Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный // Вопросы кибербезопасности. – 2014. – № 1. – С. 22–27.
5. Кибербезопасность как основной фактор национальной и международной безопасности XXI века / Ю.В. Бородакий [и др.] // Вопросы кибербезопасности. – 2014. – № 1. – С. 2–8.
6. **Туляков, О.** Информационная война в планах Пентагона / О. Туляков // Зарубежное военное обозрение. – 2015. – № 11. – С. 3–14.
7. **Колосков, С.** Стратегия действий министерства обороны США в киберпространстве / С. Колосков // Зарубежное военное обозрение. – 2016. – № 10. – С. 3–7.
8. **Сабынин, В.** Специалисты, давайте говорить на одном языке и понимать друг друга / В. Сабынин // Информост – Средства связи. – № 6.
9. **Сэйер, П.** Lloyd страхует от хакеров / П. Сэйер // Computerworld Россия. – 2000. – № 30.
10. **Хмелев, Л.С.** Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем / Л.С. Хмелев // Безопасность информационных технологий: материалы науч.-технич. конф., Пенза, июнь 2001 г. – С. 55–60.
11. **Баутов, А.** Стандарты и оценка эффективности защиты информации / А. Баутов // Стандарты в проектах современных информационных систем: материалы III Всероссийской практ. конф., Москва, 23–24 апр. 2003 г.
12. **Баутов, А.** Экономический взгляд на проблемы информационной безопасности / А. Баутов // Открытые системы. – 2002. – № 2.
13. Практические рекомендации по информационной безопасности / С. Вихорев, А. Ефимов // Jet Info. – 1996. – № 10–11.

The article considers problems of assessment of efficiency of protection of information. The authors continued the further development of the methodology of information protection issues which were raised in the journal, proposed to describe a comprehensive approach to assessing threats to information security c estimates the state of the object of protection in the event of security breach with use of private integral index of protection characterizing the ability to damage in its implementation according to which the ranking is made.

Получено 07.03.2018.