УДК 004

Методический подход к комплексному описанию объекта информационной защиты с оценкой его рисков

Рассмотрен методический подход к комплексному описанию объекта информационной защиты с оценкой его рисков. Предложено описывать данный подход, используя анализ архитектуры объекта в приложении по отношению к возможным нарушениям информационной безопасности, а также производить оценку риска с применением аппарата теории нечетких множеств.

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

С.И. ПАСКРОБКА,
канд. воен. наук, доцент,
зам. начальника научно-исследовательской части

УО «Белорусский государственный университет информатики и радиоэлектроники»

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

Ключевые слова:
информационная безопасность, защита информации, угроза безопасности, объект информационной защиты, киберпространство.

Введение. Анализ современных аналитических публикаций [1–15] показывает, что в настоящее время средства информационного воздействия и защиты развиваются наиболее динамично. Это прежде всего объясняется такими свойствами инфосферы, как неисчерпаемость и восполняемость инфоресурсов, возможность их быстрого копирования, перемещения практически без потерь на огромные расстояния с высокой скоростью и степенью достоверности, компактность источников и носителей информации, мгновенная, но бескровная реакция (отклик) инфосферы на трудноидентифицируемое в отношении источников информационное воздействие. Например, разработка и внедрение передовых технологий военного назначения является главным направлением деятельности управления перспективных исследований МО США (DARPA) [1]. Объем финансирования DARPA в этом направлении представлен на рис. 1.

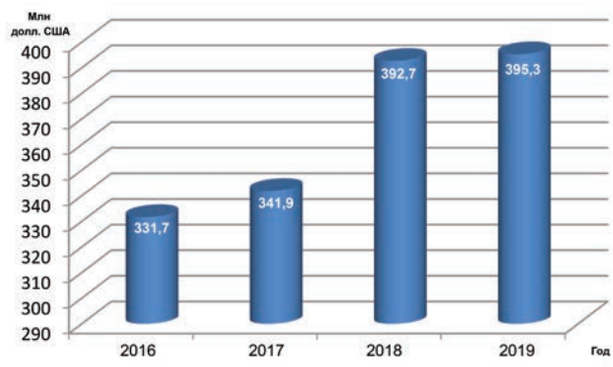


Рисунок 1– Объем финансирования управлением DARPA работ в области кибербезопасности

Развитие средств и способов ведения наступательных и оборонительных действий в киберпространстве DARPA предполагает продолжить в рамках начатого в 2018 г. проекта «Комплексные кибероперации» (Symbiotic Cyber Operations).

Значительные усилия DARPA в области киберразведки в настоящее время сконцентрированы на повышении точности и оперативности определения конкретных источников деструктивных действий в киберпространстве.

Теоретический анализ. Авторами статьи на страницах предыдущих номеров журнала [2, 3] были выработаны и предложены методические подходы к оценке вероятностей реализации угроз безопасности информации и к комплексной оценке угроз безопасности информации с оценкой состояния объекта защиты при нарушении безопасности.

На наш взгляд, для комплексного обследования и описания объекта оценки (ОО) прежде всего необходимо определиться с исходными данными.

Предлагается осуществлять данный процесс по предложенной авторами схеме, представленной на рис. 2.

В результате анализа формируются выходные данные, которые могут включать: активы, подлежащие защите; общие угрозы безопасности для анализируемого ОО; уязвимые места ОО; требования защиты.

Выходные данные процесса анализа ОО являются исходными данными для определения перечня актуальных угроз. К дополнительным исходным данным относятся требуемый уровень безопасности и метод оценки рисков. Формирование перечня актуальных для ОО угроз проводится на основании их ранжирования и сравнения с некоторым допустимым пороговым значением. Ранжирование угроз безопасности базируется на оценочном значении потенциала угрозы, который определяется категориями опасности как нарушителя безопасности, так и угрозы.

Для оценки опасности нарушителя целесообразно использовать его персональные характеристики (квалификация, мотивация и используемый ресурс), а для оценки опасности угрозы – такие параметры, как способ, цели реализации угрозы и используемое уязвимое место.

Далее необходимо оценить потенциал угроз безопасности. Это можно сделать на основании

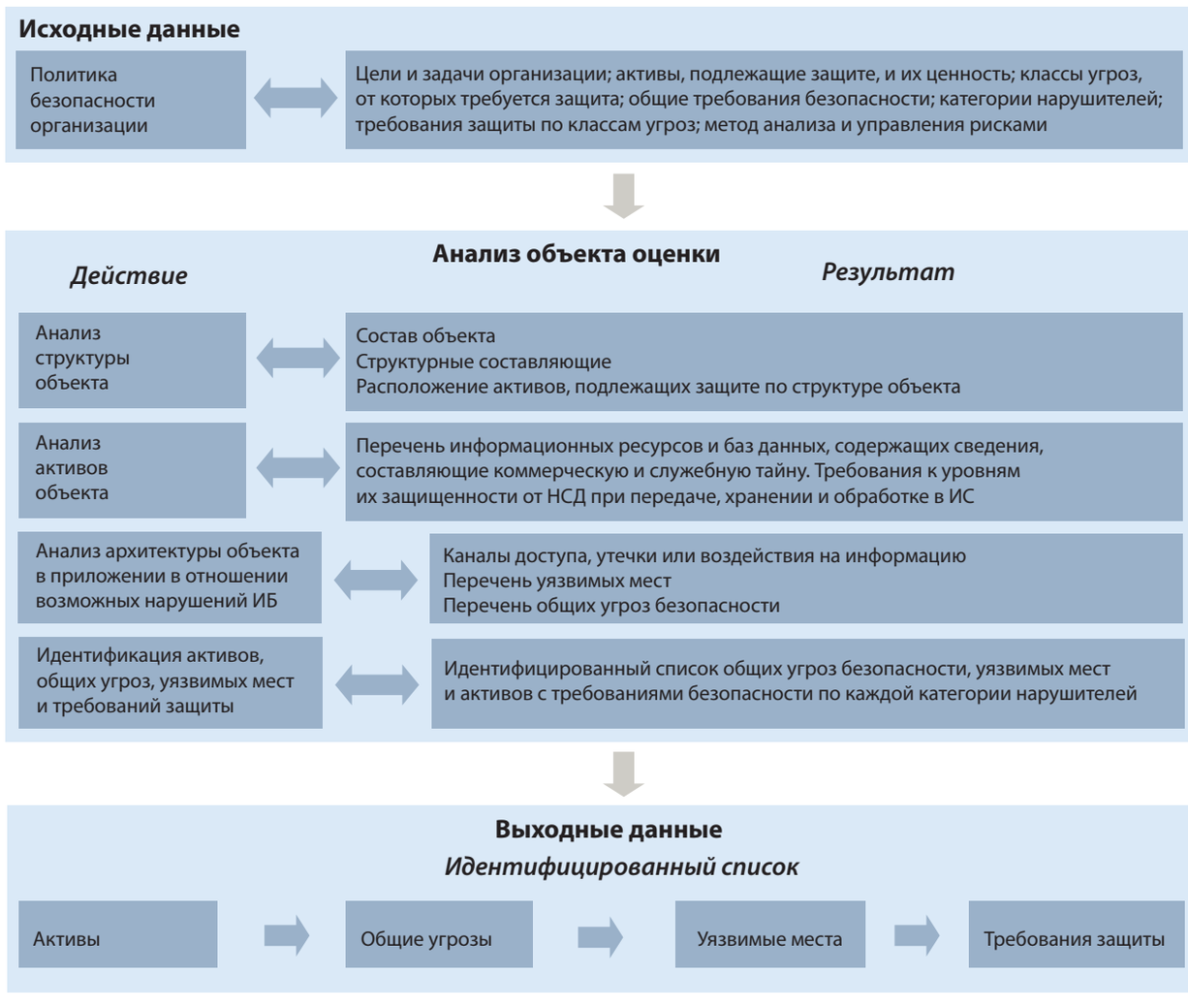


Рисунок 2 – Содержание процесса комплексного обследования и описания ОО

оценочных значений следующих факторов безопасности: актива, ущерба, вероятности реализации угрозы.

Путем сравнения рассчитанных потенциалов угроз с некоторым пороговым значением формируются перечни исключенных и актуальных угроз для данного ОО (рис. 3).

Результаты и их обсуждение. Рассуждая далее, выработаем подход к оценке риска с использованием аппарата теории нечетких множеств.

Величину возможных потерь можно оценить по следующей формуле: *ЦЕНА ПОТЕРИ* = $P_н$ × *УЩЕРБ*, где под ущербом понимается материальная стоимость актива, $P_н$ – мера, характеризующая возможность перехода в состояние нарушения ИБ. Она определяется через параметры и характеристики угроз безопасности, уязвимостей ОО и активов.

При оценке состояний ОО при нарушении ИБ с использованием нечетких множеств элементы множеств угроз безопасности $Y = \{y_i, \mu(y_i)\}$, $i = \overline{1,I}$, уязвимостей $V = \{v_k, \mu(v_k)\}$, $k = \overline{1,K}$ и активов (информации и/или ресурсов) $A = \{a_j, \mu(a_j)\}$, $j = \overline{1,J}$, характеризующих взаимодействие ОО с внешней средой, описываются нечеткими величинами $k = (k,\ \mu(k))$, где $k \in [0;1]$ – оценочное среднее значение соответствующего нечеткого коэффициента k, $\mu(k) \in [0;1]$ – функция принадлежности нечеткой величины k.

Величина риска

$$r_{ikj}\left(r^{\bullet}_{ikj}, \mu^{\bullet}_{ikj}\right) = y_i \cdot v_k \cdot a_j, \quad (1)$$

будет определяться с использованием выражений

$$r^{\bullet}_{ikj} = y_i \cdot v_k \cdot a_j, \quad \mu^{\bullet}_{ikj} = \min\left(\mu_i, \mu_k, \mu_j\right). \quad (2)$$

Ущерб j-му активу описывается формулой

$$U_j = \sum_{i,k} r_{ikj} \cdot s_j, \quad (3)$$

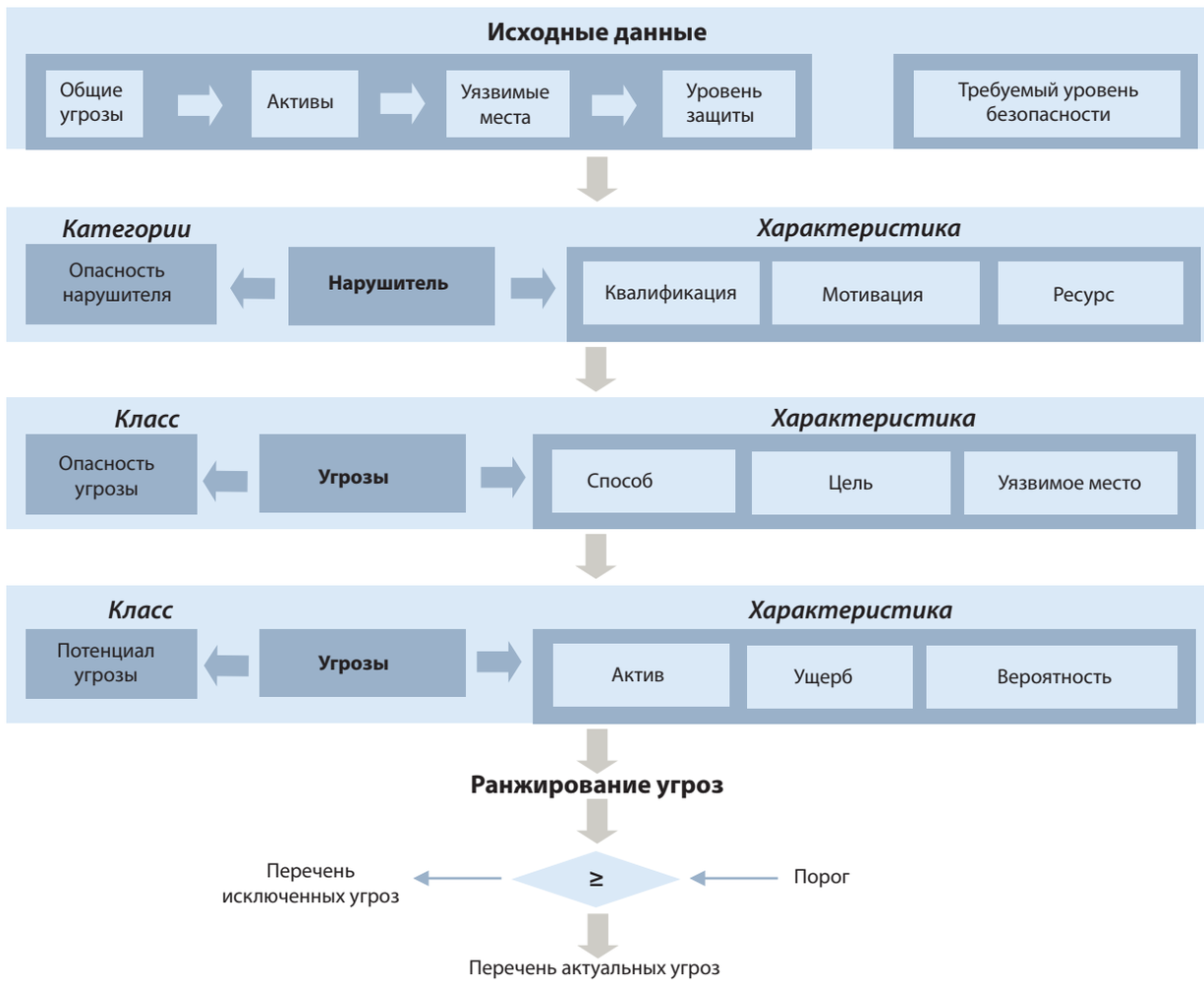


Рисунок 3 – Процесс определения перечня актуальных угроз

а суммарный ущерб – выражением

$$U = \sum_{i,k,j} r_{ikj} \cdot s_j , \quad (4)$$

где s_j – материальная ценность j-го актива.

Степень опасности угрозы y_i, оценивается по нескольким параметрам и рассчитывается по формуле

$$y_i\left(y_i, \mu_i\right) = \prod_{l=1}^{L} y_{il} = \left(\prod_{l=1}^{L} y_{il}, \min_l \left(\mu_{il}\right) \right), \quad (5)$$

где $y_{il} \in [0;1]$ – оценочное среднее значение l-го параметра i-й угрозы; $\mu_{il} \in [0;1]$ – степень принадлежности нечеткой величины y_{il} – l-го параметра i-й угрозы; L – количество параметров угрозы.

Степень опасности уязвимости v_k и значимость актива a_j оцениваются аналогично. Следует отметить, что параметры угроз, уязвимостей и активов не обязательно должны оцениваться по шкале от 0 до 1. В случае если используется другая шкала оценки параметров, необходимо провести нормировку.

Все параметры угроз, уязвимостей и активов (за исключением материальной стоимости актива) оцениваются в соответствии с приведенными выше балльными шкалами и представляются в виде нечетких величин с L = 5 термами на множестве-носителе [0; 1]. Функции принадлежности значения параметра k_i терму j представляют собой колоколообразные функции с максимумами в точках 0; 0,25; 0,5; 0,75; 1 для 1-го … 5-го термов соответственно и могут быть рассчитаны по формуле:

$$\mu_i^j\left(k_i\right) = \frac{1}{\left(1 + \left(k_i \cdot \left(L-1\right) - i + 1\right)^2\right)^{\beta}},$$

$$L = \overline{1,5}. \quad (6)$$

Для теоретической проработки подхода рассмотрим особенности реализации операции умножения нечетких величин.

Выполнение операции умножения с использованием максиминной композиции над большим количеством переменных ведет быстрому росту пар $\left(k,\ \mu(k)\right)$, задающих нечеткую величину. Так, в нашем случае в зависимости от источника угроз риск оценивается по 8 или 9 параметрам, каждый из которых после преобразования в нечеткую величину (фаззификации) описывается пятью парами $\left(k,\ \mu(k)\right)$. Риск в таком случае будет содержать до двух миллионов таких пар, что явно избыточно и требует больших вычислительных затрат.

Основываясь на принципе обобщения, максиминная композиция реализуется двумя процедурами. Первая выполняется по формуле

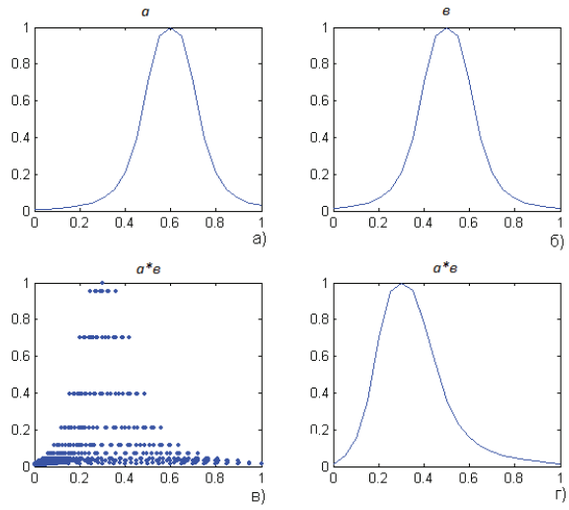
$$z = x \cdot y = \bigcup_{i=1}^{n} \left(m_x\left(x_i\right)/x_i\right) \cdot \bigcup_{j=1}^{m} \left(m_y\left(y_j\right)/y_j\right) =$$

$$= \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} \left(\left(\mu_x\left(x_i\right) \wedge \mu_y\left(y_j\right)\right)/x_i \cdot y_j \right) \quad (7)$$

Во второй процедуре осуществляется поглощение нескольких компонентов $\mu_z\left(z_k\right)/z_k, k = \overline{1,r}$ (r – количество компонентов с равнозначными носителями) одним $\mu_z\left(z_s\right)/z_s$; $\mu_z\left(z_s\right) = \max\left(\mu_z\left(z_k\right)\right)$. Результат первой процедуры можно увидеть на рисунке 4в. Вторая процедура несколько уменьшает количество полученных точек, однако оно все равно остается велико, при этом остаются точки, степень принадлежности которых заметно ниже, чем у ближайших соседей, т. е. функция принадлежности результирующего числа имеет множество провалов. Их наличие практически не влияет на конечный результат, и их можно отбросить, заменив функцию принадлежности огибающей (рисунок 4г). В результате количество пар $\left(k,\ \mu(k)\right)$ может быть уменьшено.

Получить огибающую можно, совершив операцию умножения с помощью α-уровневого принципа обобщения. Суть его заключается в следующем. Исходные числа урезаются по уровню α (т. е. из всех a_i, b_j остаются только те, для которых степень принадлежности не меньше α), вычисляются значения $a_i \times b_j$, и для всех $\min(a_i b_j) \le z \le \max(a_i b_j)$ степень принадлежности принимается равной α. Проделав эту операцию для множества α от 0 до 1 (в MatLab используется 101 значение α = 0:1 с шагом 0,01) и объединив полученные результаты аналогично второй процедуре максиминной композиции, получим искомую огибающую, значение которой с помощью интерполяции можно рассчитать для любых значений множества-носителя.

Заключение. Таким образом, предложенный методический подход позволяет получить огибающую и построить результат на любом выходном множестве-носителе с любым желаемым числом компонентов. На основании изложенных принципов можно разработать программу в среде MatLab, производящую анализ рисков при различных значениях входных переменных. Разработанный методический



а, б – нечеткие числа *a* и *b*; в – результат первой процедуры максиминной композиции при умножении чисел *a*×*b*; г – результат умножения *a*×*b*, полученный с помощью α-уровневого принципа обобщения

Рисунок 4 – Выполнение операции умножения

подход, представляющий собой содержание и взаимосвязь процедур управления ИБ на всех этапах жизненного цикла ОО, является формальным инструментом для построения частных моделей и системы управления ИБ в целом. На основании этих моделей можно разработать: методики количественной оценки защищенности; методы и подходы к описанию факторов, влияющих на защищенность; методики оценки защищенности операционных систем с использованием методологического подхода к безопасности ИС. Проведенные исследования показали необходимость продолжения работ в данном направлении.

ЛИТЕРАТУРА

1. **Баташов, В.** Деятельность министерства обороны США по развитию новых технологий в сфере кибербезопасности / В. Баташов // Зарубежное военное обозрение. – 2018. – № 10. – С. 10–13.
2. **Кулешов, Ю.Е., Паскробка, С.И., Богатырев, А.А., Касанин, С.Н.** Комплексный подход к оценке угроз безопасности информации с оценкой состояния объекта защиты при нарушении безопасности / Ю.Е. Кулешов, С.И. Паскробка, В.А. Сергиенко, С.Н. Касанин // Научно-производственный журнал «Веснік сувязі». – 2018. – № 3. – С. 45–49.
3. **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.
4. **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.
5. **Казаковцев, А.В.** НАТО и кибербезопасность / А.В. Казаковцев // Вестник Волгоградского государственного университета. – 2012. – № 2. – С. 109–114.
6. **Безкоровайный, М.М.** Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный // Вопросы кибербезопасности. – 2014. – № 1. – С. 22–27.
7. Кибербезопасность как основной фактор национальной и международной безопасности XXI века / Ю.В. Бородакий [и др.] // Вопросы кибербезопасности. – 2014. – № 1. – С. 2–8.
8. **Туляков, О.** Информационная война в планах Пентагона / О. Туляков // Зарубежное военное обозрение. – 2015. – № 11. – С. 3–14.
9. **Колосков, С.** Стратегия действий министерства обороны США в киберпространстве / С. Колосков // Зарубежное военное обозрение. – 2016. – № 10. – С. 3–7.
10. **Сабынин, В.** Специалисты, давайте говорить на одном языке и понимать друг друга / В. Сабынин // Информост – Средства связи. – № 6.
11. **Сэйер, П.** Lloyd страхует от хакеров / П. Сэйер // Computerworld Россия. – 2000. – № 30.
12. **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.
13. **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.
14. **Баутов, А.** Экономический взгляд на проблемы информационной безопасности / А. Баутов // Открытые системы. – 2002. – № 2.
15. Практические рекомендации по информационной безопасности / С. Вихорев, А. Ефимов // Jet Info – 1996. – № 10–11.

The methodical approach to the complex description of the information protection object with the assessment of its risks is considered. It was proposed to describe this approach using the analysis of the architecture of the object as applied to possible information security violations, as well as to make a risk assessment using the apparatus of the theory of fuzzy sets.

Получено 28.11.2018.