Ведищев В.В., Батищев Р.В.

Постановка задачи оптимизации выбора мер и средств защиты информации для государственных информационных систем

Аннотация: Рассмотрена задача формирования приемлемого набора защитных механизмов для государственных информационных систем с учетом динамики изменения вероятностей реализации угроз.

Ключевые слова: нечеткие числа, угроза безопасности информации, динамика реализации угроз, эффективность защиты информации

Определение средств и методов обеспечения безопасности данных оптимальным образом традиционно ставится в общем виде [1-3]. Вместе с тем, наличие неопределенности значений характеристик защищенности информации требует перехода к решению с использованием нечетких чисел [4-5], что меняет вид целевой функции, приводя ее к синтаксису, используемому для нечетких множеств. Также, следует учесть, что характеристики исполняемых угроз безопасности информации имеют динамическую природу, что влечет появление дополнительной неопределенности.

В [6] предлагается для учета неопределенностей при моделировании технологии производства перейти от точечной оценки отработанной технологии при математическом моделировании к построению законов распределения входных и выходных величин с целью сохранения целостности информации. Для полного решения задачи выбора средств и методов защиты информации возможны три подхода.

Первая постановка содержит целевую функцию оптимизации затрат на информационную безопасность при заданном уровне эффективности защиты информации [1]:

$$\left.\begin{aligned} &\eta_{ЗИ}(t) \geq \eta_{ЗИ\ зад}(t); \\ &C = \sum_{j=1}^{v} C_j \rightarrow \min \end{aligned}\right\}, \qquad (1)$$

где $\eta_{ЗИ}(t)$ – степень (уровень) защищенности информации на объекте;

$\eta_{ЗИ\,зад}(t)$ – заданное значение уровня защищенности информации на объекте;

C – стоимость комплекса элементов защиты, C_j – стоимость j-го элемента защиты.

Произведем переход от классической задачи оптимизации [1] к нечеткой постановке, где мультипликативная функция представляет собой нечеткую зависимость, рассчитываемую по формуле [4-5]:

$$\eta_{ЗИ}(t) = \prod_{u}\left\{1 - K_u(t) \circ \prod_{i_u}^{I_u}\left[\delta_{i_u} \circ P_{yi_u}(t) \circ P_{реал.i_u}(t / y_{i_u})\right]\right\} \bullet \left(K_u^{эт}(t) \to \eta^{эт}\right), \qquad (2)$$

где $K_u(t)$ – коэффициент опасности u- й угрозы, задаваемый нечетким числом;

δ_{i_u} – единичная функция, равная 1, если u-я угроза для ОИ, завершающаяся i_u- й реализацией (атакой), может иметь место для ОИ, и равна 0 в противном случае;

$P_{yi_u}(t)$ – вероятность появления за время t_u- й угрозы на ОИ, завершающейся i_u- й реализацией (атакой);

$P_{реал.i_u}(t/y_{i_u})$ – условная вероятность того, что за время t состоится i_u-я реализация угрозы (атака) при условии появления u-й угрозы. Композиция • с эталонным преобразованием $K_{\Sigma}^{эт} \to \eta^{эт}$, произведение $\prod_u$ и операция $\circ$ умножения нечетких чисел осуществляются по правилам теории нечетких множеств, что требует соответствующего изменения алгоритма.

Прямой расчет показателей реализации различных угроз безопасности требует построения зависимостей их законов распределения от законов распределения вероятностей формирования и осуществления различных угроз безопасности информации в информационных системах в предыдущие периоды [6], что приводит к учету необходимо принять следующие предположения о предметной области:

1) угроза считается актуальной в течение такого периода времени, когда она реализуется с вероятностью, близкой к единице;

2) меры защиты относятся к классу вероятностно независимых величин, их вклад в общий показатель защищенности носит интегральный характер;

3) в границах рассматриваемого интервала времени влияние меры (средства) защиты на эффективность защиты стационарно.

Интегральный показатель защищенности, в итоге, представлен в виде функции:

$$\eta(t) = f\left(\bigcup_{u=1}^{U}[\theta_{1u}, \theta_{2u}, .. \theta_{vu}]\right), \tag{3}$$

где θ_{vu} – коэффициент эффективности, показывающий, во сколько раз снижается вероятность реализации u-ой угрозы при применении v-го средства (меры) защиты. В явном виде указанная зависимость может быть представлена в следующем виде:

$$\eta(t) = \prod_{u=1}^{U}\left[1 - K_u \circ \prod_{v=1}^{V}\theta_{vu}\right] \tag{4}$$

Последовательность этапов выбора оптимального комплекса элементов СЗИ, соответствующих заданным требованиям при первой постановке задачи, приведена ниже (рисунок 1):

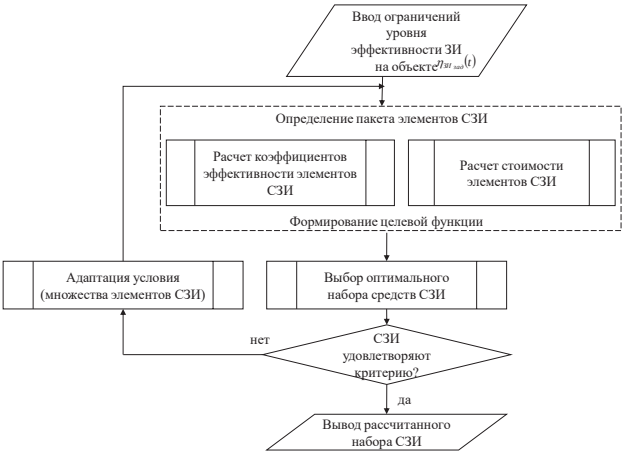

Рисунок 1 – Последовательность этапов выбора оптимального комплекса элементов СЗИ, соответствующих заданным требованиям при первой постановке задачи

Альтернативным решением является максимизация уровня защиты информации при ограничениях на стоимость решения [1]:

$$\left.\begin{array}{l} C = \sum_{j=1}^{v} C_j \le C_{зад}; \\ \eta_{ЗИ}(t) \to \max \end{array}\right\}, \qquad (5)$$

где C – стоимость комплекса элементов защиты;

C_j – стоимость j -го элемента защиты;

$C_{зад}$ – заданная стоимость комплекса элементов защиты;

$\eta_{ЗИ}(t)$ – степень защищенности информации на объекте, при применении средств защиты.

Последовательность решения данной задачи соответствует предыдущей, с отличием вида целевой функции и ограничений и является «обратной» задачей математического программирования (рисунок 2).

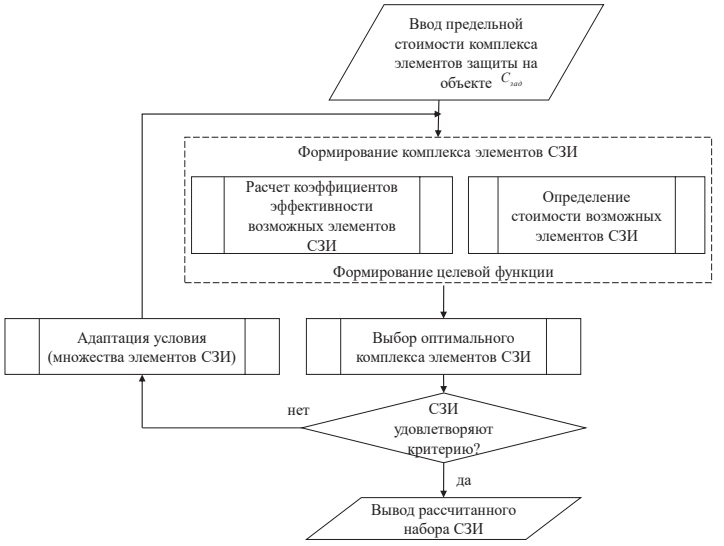

Рисунок 2 – Последовательность этапов выбора оптимального комплекса элементов СЗИ, соответствующих заданным требованиям при второй постановке задачи

Однако, при решении практических задач обеспечения информационной безопасности, конкретные значения коэффициента эффективности и соответствие конкретным критериям не требуется. Задается класс защищенности по приказу ФСТЭК от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [7], который должна обеспечивать разрабатываемая СЗИ. С целью соответствия принятому порядку определим третью постановку задачи обоснования требований к СЗИ, в которой определяются комплексы мер и средств защиты по заданному классу защищенности [7]:

$$\bigcup_{\nu} S_{\nu}\{\theta_1, \theta_2, ..., \theta_u\} \rightarrow K_{П} \qquad (6)$$

где $K_{П}$ – класс защищенности по Приказу [7];

$S_\nu\{\theta_1,\theta_2..\theta_u\}$ – ν -й компонент (мера, средство) в составе СЗИ с соответствующими коэффициентами эффективности.

Первоначально, при разработке СЗИ задается класс защищенности по Приказу [7], который проектируемая система должна обеспечивать. По списку требований класса защищенности из множества возможных способов и средств защиты определяется комплекс элементов СЗИ, который способен удовлетворять этому классу. Значение коэффициента эффективности защиты рассчитывается для каждого элемента будущей СЗИ.

Далее осуществляется формирование комплексов сочетаемых элементов СЗИ, с учетом возможного повтора функционала и ограничений на условия применения. Первичное решение будет содержать комплекс элементов СЗИ с максимальным коэффициентом защищенности, что обеспечит соответствие требуемому классу защиты.

Перебор всех альтернатив комплектования СЗИ предоставит множество допустимых по критерию соответствия решений требованиям по обеспечиваемому классу защиты, заданному на первом этапе. При этом, значение коэффициента защищенности информации каждого комплекса СЗИ будет разным, что позволит выбрать оптимальный вариант из множества предложенных, учитывая также затраты на его реализацию.

Заключение

Обеспечение информационной безопасности с помощью эффективно подобранного комплекта СЗИ позволит сэкономить ресурсы при строгом соответствии требуемому классу защиты.

Литература:

1. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных: в 2 кн. Книга 1. – Москва: Энергоатомиздат, 1994. – 400 с.

2. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных: в 2 кн. Книга 2. – Москва: Энергоатомиздат, 1994. – 175 с.

3. *Юдин Д.Б., Гольштейн Е.Г.* Линейное программирование (теория и конечные методы). – Москва: Физматгиз, 1963. – 775 с.

4. *Жижелев А.В., Панфилов А.П., Язов Ю.К., Батищев Р.В.* К оценке эффективности защиты информации в

телекоммуникационных системах посредством нечетких множеств. // Известия высших учебных заведений. Приборостроение. – 2003. – Т. 46. № 7. – С. 22-29.

5. *Язов Ю.К., Батищев Р.В., Кулаков В.Г., Остапенко Г.А., Ференец С.С.* К вопросу о расчете комплексного показателя угроз информации на объекте информатизации // Информация и безопасность. – 2003. – Т. 6. № 2. – С. 80-81.

6. *Ведищев В.В., Батищев Р.В.* Вероятностный подход при управлении технологией как фактор повышения уровня информационной безопасности производства листового проката / Проблемы управления безопасностью сложных систем: материалы XXXI международной конференции (Москва, 13 декабря 2023 года). – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2023. – С. 256-261. – DOI 10.25728/iccss.2023.89.10.034. – URL: https://elibrary.ru/item.asp?id=59824072&pff=1 (дата обращения 10.10.2024).

7. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 Федеральная служба по техническому и экспортному контролю «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Фесенко Д.Е.

Обоснование Проекта разработки Карты градостроительных рисков применительно к актуальным военно-стратегическим условиям в РФ

Аннотация: В Обосновании Проекта разработки Карты градостроительных рисков применительно к актуальным военно-стратегическим условиям членами Ассоциации «Стратегия 50» предлагается классифицировать эти риски: по географии, по месту и значимости поселений, по характеру объектов, по типологии зданий и сооружений и др., выразив в балльной форме. Соответственно