6. *Путивцев М. Е., Баранник А. А*. Модель проведения сертификации по стандарту ISO\IEC 17799 с использованием процессного подхода. – Таганрог: Технологический институт ЮФУ, 2007.

7. Что такое RACI model? *Источник: http://www.12manage.com/methods_raci_ru.html*

УДК 681.324

И.В. Машкина, С.Н. Алекса

РАЗРАБОТКА МЕТОДА И ФУНКЦИОНАЛЬНОЙ МОДЕЛИ ЧИСЛЕННОЙ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ НА ОСНОВЕ ВЕРОЯТНОСТНО-СТАТИЧЕСКОГО ПОДХОДА*

Адекватный научно-методологический базис должен содержать количественные методы анализа и синтеза систем защиты и управления ими в процессе функционирования. Потому одним из основных положений унифицированной концепции защиты [1] является требование научно обоснованного подхода к оценке, желательно в количественном выражении, требуемого уровня защищенности (риска) на объекте защиты в изменяющихся условиях его функционирования.

Процесс оценивания величины риска нарушения информационной безопасности (ИБ) при проектировании системы защиты информации (СЗИ) включает в себя: определение ценности ресурсов, изучение угроз и уязвимостей, выбор параметров для их описания и получение оценок вероятностей по этим параметрам, оценок теоретической эффективности контрмер и ожидаемого ущерба, определение его приемлемости.

В процессе анализа и оценивания рисков устанавливается степень адекватности используемых или планируемых наборов средств защиты (СрЗ) существующим угрозам. Свойство защищенности информации каждого СрЗ, входящего в СЗИ, в совокупности определяет защищенность информации в СЗИ в целом.

Наличие уязвимости СрЗ может привести к нарушению защищенности, т. е. осуществлению угрозы. При решении задач защиты информации первостепенное значение имеет количественная оценка ее уязвимости. Поскольку воздействие на информацию различных факторов в значительной мере является случайным, то в качестве количественной меры ее уязвимости наиболее целесообразно применить вероятность нарушения защищенности информации $P_{бт}^{н}$.

Неясность способа определения значений вероятностей угроз и уязвимостей является основной проблемой при получении количественной оценки риска нарушения ИБ. Известно, что применение методов классической теории вероятностей допустимо при повторяемости опытов и одинаковости условий. Это требование в сложных системах, какими являются СЗИ, обычно не выполняется.

Значение показателя СрЗ защищенности информации $P_{бт}$ – это *субъективная вероятность* обнаружения и блокирования СрЗ несанкционированных действий, т. е. теоретическая ожидаемая эффективность барьера.

Очевидно, *вероятность нарушения защищенности* $P_{бт}^{н}$ дополняет $P_{бт}$ до единицы т.е.

*Работа выполнена при поддержке гранта РФФИ №08-08-97035.

$$P_{бт}^{н} = 1 - P_{бт}, \quad (1)$$

где $P_{бт}^{н}$ – вероятность нарушения защищенности информации, или вероятность уязвимости m-го СрЗ (вероятность преодоления барьера).

Методы оценивания СрЗ разделяются на качественные и количественные. Качественные методы используются на начальных этапах моделирования. С этой целью была разработана система иерархических критериев качества СрЗ, относящихся к следующим функциональным подсистемам: VPN, МСЭ. IDS, антивирусная защита, сетевой контроль доступа, обнаружение вторжений на хосте, разграничение доступа, резервное копирование и др.

В работе решается задача получения численной оценки обобщенного показателя качества СрЗ. Численное оценивание заключается в сопоставлении обобщенному показателю качества СрЗ защищенности информации – одного числа. Эта задача может быть решена с помощью экспертов. При этом оценка значений субъективных вероятностей $P_{бт}$, должна быть свободна от произвола. Частные показатели защищенности должны иметь ясный физический смысл и быть взаимосвязанными. Поэтому особенностью предлагаемого в работе подхода является получение численных оценок субъективных вероятностей $P_{бт}$ на основе объективных технических характеристик и возможностей СрЗ, декларируемых их разработчиками.

В настоящее время все чаще для получения решений в области ИБ используется математический аппарат нечетких множеств. В работе рассматривается использование аппарата нечетких множеств для получения численной оценки обобщенного показателя качества СрЗ – защищенность информации.

Функции принадлежности (ФП) были сформированы для оценки СрЗ по каждому критерию нижнего иерархического уровня. Использовались известные методы построения ФП, основанные на формализации и интеграции нечетких данных, сформированных экспертом в процессе оценивания параметров реальных СрЗ. Сформулированы соответствующие продукционные правила, позволяющие обрабатывать сложные соединения.

Достоинство способа – относительно высокая объективность. Субъективные моменты в оценку полезности хотя и вносятся, но не прямо, как при других способах, а косвенным образом.

В вероятностно-статическом подходе не учитывается динамика изменения значений вероятностей угроз и уязвимостей во времени, оцениваются априорные *ожидаемые значения вероятностей* нарушения защищенности информации.

Предлагаемый метод оценивания уровня защищенности объекта защиты (ОЗ) базируется на трехрубежной модели СЗИ, описанной в [2].

Известно, что *уровень защищенности* и относительный риск дополняют друг друга до единицы. Будем рассчитывать уровень защищенности η по формуле [3]:

$$\eta = 1 - \overline{R} = 1 - \sum_{S} \frac{C_s}{C_\Sigma} \cdot P_s, \quad (2)$$

где $\overline{R}$ – относительный риск нарушения ИБ, C_s – доля стоимости защищаемых информационных ресурсов в сегменте, s – номер сегмента, S – число сегментов, P_s – результирующая вероятность угроз информационной среде сегмента, C_Σ –

суммарный неприемлемый ущерб, $\frac{C_s}{C_\Sigma}$ – коэффициент опасности совокупности угроз в s-м сегменте, определяемый как доля стоимости защищаемой информации ОЗ, обрабатываемой в сегменте.

Таким образом, для оценки уровня защищенности требуется количественная оценка вероятностей реализации каналов несанкционированного доступа.

Приведем возможный вариант математического анализа ИБ ОЗ, который представляет собой сегментированную сеть, для случая, когда в разных сегментах обрабатывается информация различной степени важности (критичности).

Общее выражение для вероятности нарушения защищенности подмножеством нарушителей {K'} по подмножеству представляющих интерес каналов несанкционированного получения информации {J'} для сегмента s имеет вид [1]:

$$P_{S\{J'\}\{K'\}} = 1 - \prod_{J'} \left(1 - P_{sjk}^{(б)}\right) \prod_{K'} \left(1 - P_{sjk}^{(б)}\right). \quad (3)$$

Обозначим $P_{sjk}^{(б)внш}$ – вероятность несанкционированного получения информации, обрабатываемой в s-м сегменте, внешним нарушителем, считая, что на ОЗ есть точки выхода из системы в глобальную сеть, внешние выделенные каналы связи, т. е. возможны удаленные атаки через периметр; $P_{sj}^{(б)вн}$ – вероятность нарушения конфиденциальности информации, обрабатываемой в s-м сегменте, внутренним нарушителем.

Тогда

$$P_{sjk}^{(б)внш} \subset P_{sjk}^{(б)}, P_{sj}^{(б)вн} \subset P_{sjk}^{(б)}. \quad (4)$$

С учетом принятой трехрубежной модели защиты $P_{sjk}^{(б)внш}$ может быть определена по формуле

$$P_{sjk}^{(б)внш} = 1 - \prod_{l=1}^{3} (1 - P_{sjkl}^{внш}), \quad (5)$$

где $P_{sjkl}^{внш}$ – вероятность нарушения конфиденциальности информации, обрабатываемой к s-м сегменте, внешним нарушителем в случае преодоления соответствующего рубежа защиты (РЗ) *l*. Вероятность $P_{sjkl}^{внш}$ зависит от четырех факторов, поэтому определяется зависимостью

$$P_{sjkl}^{внш} = P_{skl}^{д} \cdot P_{sjkl}^{н} \cdot P_{sjl}^{к} \cdot P_{sjl}^{и}, \quad (6)$$

где $P_{skl}^{д}$ – вероятность попытки доступа злоумышленника или внешнего нарушителя к *l*-му РЗ (границе сети – периметру, границе сегмента, к хосту), принимается в расчетах равной 1; $P_{sjkl}^{н}$ – вероятность преодоления злоумышленником или

внешним нарушителем *l*-го РЗ; $P^{к}_{sjl}$ – вероятность проявления канала связи s-го сегмента на РЗ *l* , зависит от технологии обработки информации на ОЗ; $P^{и}_{sjl}$ – вероятность наличия защищаемой информации s-го сегмента на *l*-м РЗ в момент доступа, зависит от технологии обработки информации на ОЗ.

Внутренний нарушитель в процессе реализации каналов несанкционированного доступа должен преодолеть два РЗ.

Тогда вероятность несанкционированного получения информации, обрабатываемой в сегменте s внутренним нарушителем, может быть вычислена по формуле

$$P^{(б)вн}_{sj} = 1 - \prod_{l=1}^{2} (1 - P^{вн}_{sjl}), \tag{7}$$

где

$$P^{вн}_{sjl} = P^{д}_{sl} \cdot P^{н}_{sjl} \cdot P^{к}_{sjl} \cdot P^{и}_{sjl}, \tag{8}$$

где $P^{д}_{sl}$ – вероятность попытки доступа внутреннего нарушителя к соответствующему РЗ *l*, принимается в расчетах равной 1; $P^{н}_{sjl}$ — вероятность доступа внутреннего нарушителя к каналу связи s-го сегмента, равная вероятности преодоления барьеров на РЗ *l*; $P^{к}_{sjl}$ — вероятность проявления канала связи на РЗ; $P^{и}_{sjl}$ — вероятность наличия защищаемой информации s-го сегмента на РЗ в момент доступа нарушителя.

Количественная оценка уязвимости СрЗ имеет первостепенное значениё в практических расчетах. В качестве количественной меры уязвимости наиболее целесообразно принять вероятность нарушения защищенности. Из перечисленных вероятностей, входящих в формулу для расчета вероятностей нарушения конфиденциальности $P^{внш}_{sjkl}$ и $P^{вн}_{sjl}$, одна из вероятностей, а именно $P^{н}_{sjkl}$ ($P^{н}_{sjl}$), зависит от качества используемых в системе СрЗ и количества барьеров на РЗ.

Если нарушителю необходимо преодолеть М барьеров па РЗ, то вероятность его удачной атаки определяется как произведение:

$$P^{н}_{sjkl} = \prod_{m=1}^{M} P^{н}_{бm}, \tag{9}$$

где $P^{н}_{бm}$ – вероятность преодоления m-го барьера, или вероятность (уровень) уязвимости СрЗ.

С учетом (1) перепишем соотношение (9) в виде

$$P^{н}_{sjkl} = \prod_{m=1}^{M} (1 - P_{бm}) \tag{10}$$

Оценив значения вероятностей $P_{б\,m}$ – показатель защищенности информации каждого СрЗ, можно будет оценить граничные значения вероятностей реализации каналов несанкционированного доступа.

Таким образом, сущность метода сводится к реализации алгоритма:

1. Для каждого сегмента составляются списки путей угроз в соответствии с принятой политикой безопасности и числом точек входа в систему.

2. Задаются численные значения ценности информационных активов в сегментах C_S.

3. Вычисляются с использованием механизма нечеткой логики показатели «защищенность информации» $P_{б\,m}$ для каждого m-го СрЗ, установленного на периметре, границах сегментов, на хостах.

4. Вычисляются и/или задаются вероятности $P^{д}_{sk\,l}$, $P^{д}_{sl}$, $P^{н}_{sjk\,l}$, $P^{н}_{sj\,l}$, $P^{к}_{sj\,l}$, $P^{и}_{sjl}$ для каждого РЗ, причем $P^{н}_{sjk\,l}$ ($P^{н}_{sj\,l}$) – вероятность преодоления барьеров на РЗ вычисляется в зависимости от числа СрЗ на рубеже по формуле (10).

5. Вычисляются вероятности для каждого из трех РЗ $P^{внш}_{sjk\,l}$ и $P^{вн}_{sj\,l}$ по формулам (6) и (8).

6. Вычисляются базовые вероятности несанкционированного получения информации, обрабатываемой в s-м сегменте, внешним нарушителем, реализующим удаленную атаку, или внутренним нарушителем, реализующим межсегментную атаку, $P^{(б)внш}_{sjk}$ и $P^{(б)вн}_{sj}$ соответственно по формулам (5) и (7).

7. Вычисляется общее выражение для вероятности нарушения защищенности s-го сегмента подмножеством нарушителей {K'} по подмножеству каналов {J'} несанкционированного получения информации по формуле (3).

8. Вычисляется уровень защищенности на ОЗ по формуле (2).

На рис. 1-4 представлены разработанные IDEF0-диаграммы модели оценивания рисков нарушения ИБ.

В настоящее время все большую популярность приобретают инженерные методы исследования на основе современных информационных технологий. В данной работе сделана попытка расширить спектр компьютеризованных инструментальных методов анализа с использованием технологии IDEF0 на процесс оценивания риска нарушения ИБ на объекте информатизации.

Разработка моделей оценки риска нарушения ИБ в стандарте IDEF0 позволяет наглядно и эффективно отобразить весь механизм оценивания в нужном разрезе.

Реализация процессов, отображаемых моделью, осуществляется с помощью автоматизированной системы, в которой реализован разработанный метод, экспертов в области ИБ, а также инструментария Fuzzy Toolbox программного продукта Matlab.

Рис. 1. Контекстная диаграмма IDEF0- модели оценивания риска нарушения ИБ

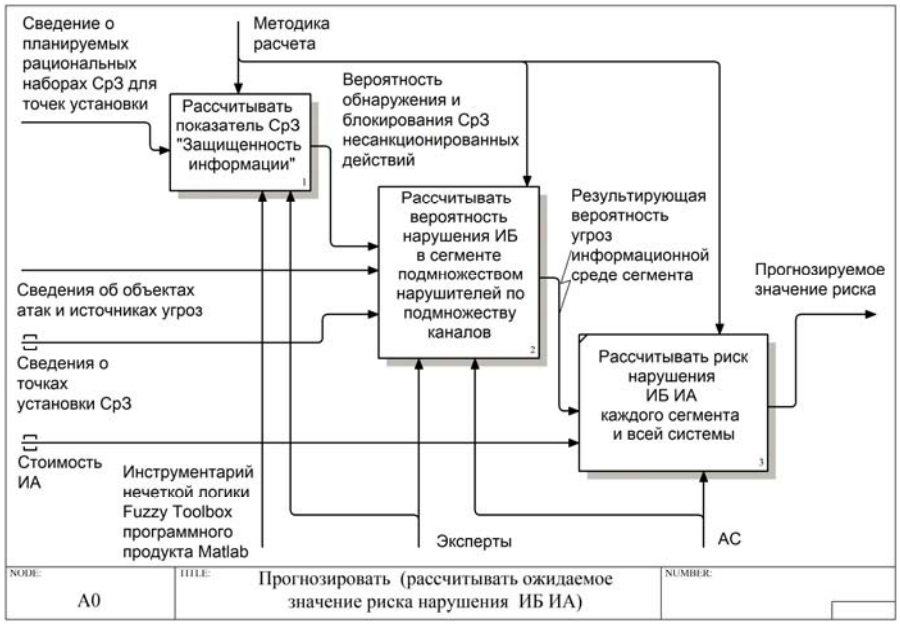

Рис. 2. Результат декомпозиции контекстной диаграммы

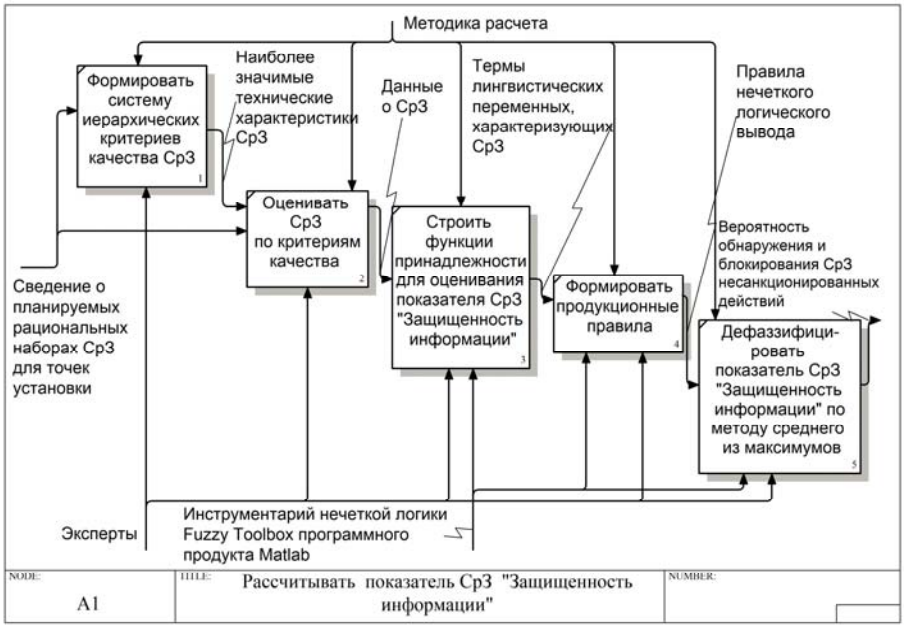

Рис. 3. Результат декомпозиции функционального блока «Рассчитывать показатель средств защиты «Защищенность информации»

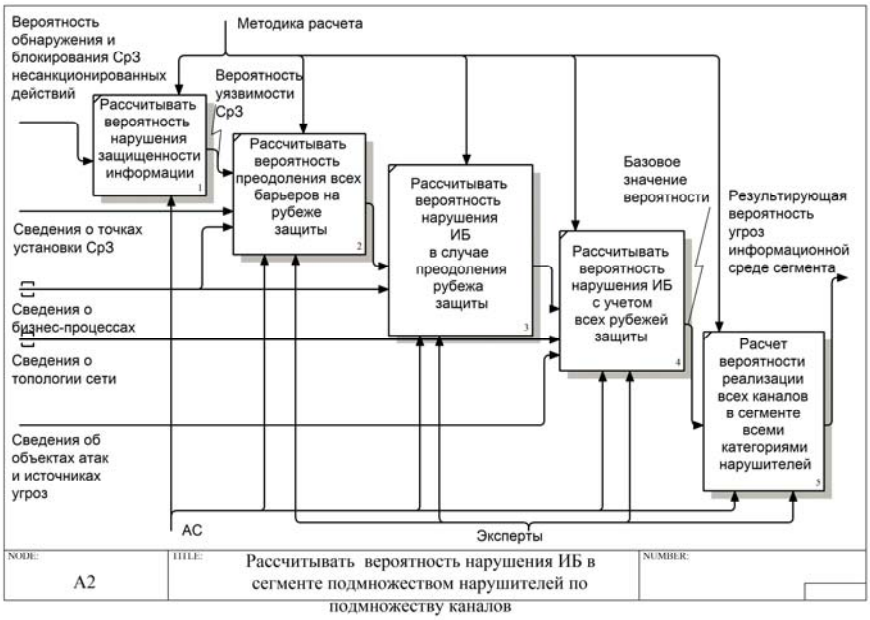

Рис.4. Результат декомпозиции функционального блока «Рассчитывать вероятность реализации каждого канала НСДУВ в сегменте»

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Малюк А.А*. Информационная безопасность и методологические основы защиты информации: Учеб. пос. для вузов. – М.: Горячая линия – Телеком, 2004. – 280 с.

2. *Машкина И.В., Васильев В.И., Рахимов Е.А.* Проектирование системы защиты информации объекта информатизация // Информационные технологии. 2006. 21. 10. – С. 17 – 26.

3. *Мирошников В.В.* Методический подход к оценке эффективности способов защиты информации в среде распространения сигналов глобальной вычислительной сети II Известия ТРТУ. Тематический выпуск: Материалы УИ Международной научно-практической конференции «Информационная безопасность». – Таганрог, 2005. – М., – №4 (48). – 250 с.