УДК 004.056.53

© 2016 г. **Н.И. Сельвесюк**, д-р техн. наук,
**А.С. Островский,** канд. техн. наук
(Московский государственный технический университет им. Н.Э. Баумана),
**В.Д. Сливинский**, канд. техн. наук
(Московский государственный лингвистический университет)

# МЕТОДОЛОГИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ*

В развитие методологии, разработанной в Институте системного анализа РАН, предлагаются метод определения критических компонентов автоматизированной системы обработки информации, а также метод определения значимых мер по предотвращению возникновения информационных рисков, позволяющие построить оптимальные модели защиты этих систем.
***Ключевые слова:*** автоматизированные системы обработки информации, информационная безопасность, анализ защищенности систем.

## Введение

При решении ряда задач, связанных с разработкой, изготовлением и развертыванием автоматизированных систем обработки информации (АСОИ), возникает необходимость обеспечения их защищенности от внешних угроз. Существующие меры и способы защиты позволяют осуществлять противодействие большинству угроз, однако их использование предполагает увеличение затрат на применение АСОИ и задействование ее вычислительных ресурсов. Таким образом, возникает противоречие между необходимостью обеспечения наиболее полной защищенности АСОИ от внешних угроз и повышением затрат на их применение при использовании полного комплекса мер и способов защиты. Следовательно, задача построения оптимальной модели защиты системы от внешних угроз, связанная с определением критических компонентов АСОИ и формированием мер по предотвращению информационных рисков, является актуальной.

Широкое внедрение современных АСОИ влечет за собой появление новых рисков, связанных с использованием информационных и компьютерных технологий. В Институте системного анализа Российской академии наук разработана ме-

* Работа выполнена при финансовой поддержке РФФИ (гранты № 14-08-00640а, 16-08-00311а).

тодология [1], позволяющая оценить возникающие риски. Данная методология основана на ассоциации АСОИ с некоторым множеством событий рисков, которые могут произойти в силу недостаточной надежности и безопасности используемых компьютерных, информационных и организационных технологий. Предлагается использовать указанную методологию для разработки методов определения критических компонентов АСОИ и значимых мер по предотвращению возникновения информационных рисков, позволяющих решить актуальную задачу построения оптимальной модели защиты системы от внешних угроз.

Любое событие риска может быть представлено как результат реализации некоторого множества угроз, связанных с недостаточной безопасностью используемых средств и технологий. Каждую угрозу можно связать с каким-либо объектом, процессом или технологией данной автоматизированной системы, т.е. с некоторым компонентом системы. Назовем существенной ту угрозу, реализация которой может привести к возникновению какого-либо события риска. Тогда для принятия решений по повышению безопасности необходимо выделить те компоненты автоматизированной системы, с которыми можно связать некоторые существенные угрозы, а затем рассчитать «вклад» каждой существенной угрозы и каждого компонента автоматизированной системы. В результате у разработчиков АСОИ появляется возможность, проанализировав все известные события риска, выявить критические компоненты системы, т.е. те ее компоненты, которые в силу недостаточной безопасности могут стать источниками событий рисков.

С каждым таким элементом системы и соответствующими ему угрозами можно связать некоторое множество возможных мер защиты и противодействия этим угрозам, принимаемых по отношению к данному элементу. Путем анализа того, как изменятся параметры событий риска в случае применения каждой из рассматриваемых мер, должны быть получены новые значения этих параметров.

На основании данных оценок определяются частный и общий рископонижающие потенциалы возможных мер защиты, которые характеризуют величину снижения ожидаемых потерь в случае применения данной меры. Те меры, рископонижающий потенциал которых превышает затраты на их осуществление, определяются как значимые. Множество значимых мер защиты образует оптимальную модель защиты АСОИ.

## Метод определения критических компонентов автоматизированных систем обработки информации

Пусть дана некоторая система $S$, которая может быть представлена в виде некоторого множества составляющих ее компонентов, с каждым из которых может быть ассоциировано некоторое множество угроз нарушения безопасности

$$S = \{O_i\}. \quad (1)$$

Как правило, любая система может быть структурирована таким образом, что в ней могут быть выделены уровни иерархии. При этом уровень системы в целом будет соответствовать 1-му уровню иерархии. В этом случае систему можно представить в виде структурной модели

$$S = \left\{O_i^j\right\}, \tag{2}$$

где верхний индекс *j* указывает иерархический уровень, на котором находится компонент. В дальнейшем этот индекс будет использоваться только в тех случаях, когда имеет значение иерархическое положение компонента.

Помимо того, что отдельные компоненты множества $\{O_i\}$ могут принадлежать разным иерархическим уровням, существует условие: если компонент находится на более высоком уровне иерархии, он может включать в себя компоненты более низкого иерархического уровня. Например, компоненты низшего уровня могут быть объединены в подсистемы. Для подсистем, в свою очередь, можно определить новое множество угроз, причем ни одну из угроз, входящих в это множество, нельзя отнести к какому-либо компоненту подсистемы. Подсистемы могут быть объединены в более крупные группы, – например, в локальные среды, и для них, в свою очередь, могут существовать угрозы, которые невозможно отнести ни к одному из входящих в них компоненту. И так далее — до уровня системы в целом.

Если для всей системы можно определить некоторое множество угроз, которое не может быть отнесено ни к одному из ее компонентов в отдельности, то в этом случае саму систему можно идентифицировать в качестве компонента множества $\{O_i\}$. Все множество угроз *Y*, связанных с системой *S* и со всеми ее компонентами, может быть представлено как

$$Y = \left\{Y^{O_i}\right\}. \tag{3}$$

Каждому объекту $O_i$ сопоставляется некоторое множество угроз $Y^{O_i}$.

Определим для системы *S* множество событий риска *R* нарушения ее безопасности. Если множество *Y* определено достаточно полно, то любое событие $r_m \in R$ может быть представлено как результат реализации некоторого множества угроз $Y_m \subseteq Y$.

Каждое событие риска $r_m$ имеет три основных количественных характеристики, определяемых исходя из экспертных оценок: $c_m$ – цену события риска – оценку ущерба, который может быть нанесен системе *S* событием риска $r_m$; $p_m$ – вероятность события $r_m$; $\nu_m$ – рискообразующий потенциал, рассчитываемый по формуле [1]

$$\nu_m = c_m \times p_m. \tag{4}$$

При этом вероятность $p_m$ события риска $r_m$ может быть рассчитана как произведение вероятностей реализации каждой из угроз множества $Y_m$ [1]

$$p_m = \prod_{n=1}^{N^{Ym}} p_n^{r_m}, \tag{5}$$

где $N^{Y_m}$ – количество угроз множества $Y_m$.

Поскольку событие риска есть результат одновременной реализации множества угроз $Y_m$, то можно говорить, что это множество угроз в рамках системы *S*

обладает совокупным рискообразующим потенциалом $v_m$. Рискообразующий потенциал каждой из угроз, входящих в множество $Y_m$, предлагается рассчитывать по формуле [1]:

$$q_m = \frac{v_m}{N^{Y_m}}. \qquad (6)$$

Данная формула отражает следующий очевидный факт: если хотя бы одна из угроз не реализована, то событие $r_m$ не осуществляется. Т.е. либо не происходит никакого события риска, либо это совсем другое событие, с совершенно иными показателями цены риска, вероятности этого события и величины риска по этому событию. Поэтому (в рамках данной модели) естественно предположить, что «вклад» каждой угрозы в событие риска, измеряемый ее рискообразующим потенциалом, одинаков и может быть рассчитан по формуле (6).

При построении всех событий из множества $R$ любая угроза $y_l \in Y$ может войти в качестве рискообразующей сразу в несколько событий риска, т.е. в некоторое подмножество $R_l$ множества событий $R$ ($R_l \subseteq R$). Соответственно имеет смысл определить для нее множество значений ее рискообразующего потенциала $Q_l$ по каждому из событий риска.

В общем случае может быть построено неограниченно большое количество событий риска, в которых каждая из угроз играет какую-то рискообразующую роль. Но, с точки зрения оценки информационных рисков, значение имеют только такие события риска, которые помогают определить реальную значимость той или иной угрозы нарушения безопасности системы $S$. Очевидно, что реальная значимость угрозы $y_l$, т.е. ее системный рискообразующий потенциал, определяется максимальным значением ее рискообразующих потенциалов по всем событиям риска $R_l$ [1]

$$q_l^S = \max_{n=1}^{N^{Q_l}} Q_l, \qquad (7)$$

где $N^{Q_l}$ – количество событий риска, в которых в качестве рискообразующей участвует угроза $y_l$.

Поскольку каждая из угроз соотнесена с некоторым компонентом системы $S$ и каждому из компонентов $O_i$ соответствует множество угроз $Y^{O_i}$, то для любого из объектов $O_i$, который не включает в себя компонентов более низкого уровня иерархии, рискообразующий потенциал рассчитывается по формуле [1]:

$$\omega^{O_i} = \sum_{n=1}^{N^{O_i}} q_n^{O_i}, \qquad (8)$$

где $N^{O_i}$ – количество угроз множества $Y^{O_i}$; $q_n^{O_i}$ – системные рискообразующие потенциалы угрозы $y_n \in Y^{O_i}$.

Если компонент $O_i$ $j$-го иерархического уровня включает множество компонентов $j + 1$ уровня иерархии

$$O_i^j \supset \{O_z^{j+1}, z = 1,..., Z^{O_i^J}\},$$

то его рискообразующий потенциал рассчитывается как сумма рискообразующего потенциала угроз для этого компонента и сумма рискообразующих потенциалов угроз для компонентов, входящих в его состав [1]:

$$\omega^{O_i^j} = \sum_{n=1}^{N^{O_i}} q_n^{O_i^j} + \sum_{z=1}^{Z^{O_i^J}} \omega_z^{O_i^{j+1}}, \qquad (9)$$

где $Z^{O_i^J}$ – количество компонентов уровня $j + 1$, входящих в компонент $O_i^j$.

Если при оценке таких параметров как цена риска и вероятность события риска определять их как показатели, относимые к одному году, а цену риска указывать в конкретных денежных единицах, то понятие рискообразующего потенциала будет отражать ожидаемые среднегодовые потери для системы в оцениваемой конфигурации в конкретных условиях ее функционирования по каждому ее компоненту, по каждой структурной составляющей и по системе в целом.

Для определения критических составляющих необходимо рассчитать вектор критичности по компонентам $\Omega^{O_i^j}$. Первоначально задается уровень критичности $\Omega$ по системе. При использовании стоимостных оценок это сумма годового ущерба, которая может считаться приемлемой для данной системы в целом. Вектор критичности по компонентам рассчитывается как совокупность показателей уровня критичности по каждому компоненту путем деления уровня критичности по модели на число компонентов структурной модели, с учетом коэффициента допустимости по отдельным компонентам:

$$\Omega^{O_i} = \frac{b^{O_i}\Omega}{\sum_{n=1}^{K} b^{O_n}}, \qquad (10)$$

где $b^{O_i}$ – коэффициент допустимости компонента $O_i$; $K$ – число компонентов системы (1).

Обычно $b^{O_i}$ полагается равным 1. Для отдельных компонентов порог критичности можно увеличивать или уменьшать в зависимости от их важности путем задания соответствующего значения $b^{O_i}$.

Те компоненты $O_i$, для которых $\omega^{O_i} > \Omega^{O_i}$, идентифицируются как критические.

## Метод определения значимых мер по предотвращению возникновения информационных рисков

Для выявления наиболее значимых мер по предотвращению возникновения информационных рисков вводится понятие потенциала снижения риска, или рископонижающего потенциала [2]. Любая мера защиты $d_k$ обладает частным потенциалом $\overline{q_l^k}$ снижения риска некоторой угрозы $y_l$, а также общим потенциалом

снижения риска $\overline{q^k}$ всех угроз, парируемых данной мерой. Частный рископонижающий потенциал меры есть выражение значимости меры по отношению к данной угрозе. Очевидно, что значимостью могут обладать только те меры, которые относятся к существенным угрозам, поэтому в дальнейшем речь идет только о таких мерах. Для того, чтобы определить общий потенциал снижения риска данной мерой, необходимо выполнить следующие действия.

На основании описания события риска нужно получить новые экспертные оценки того, как снизятся цена риска $c_m$ и вероятность события риска $p_m$, если эта мера будет принята. Разница между показателями величины рискообразующего потенциала угрозы до принятия меры $d_k$ и после ее принятия представляет собой показатель частного потенциала снижения риска данной меры при данном воздействии

$$\overline{q_l^k} = q_l^{пред} - q_l^{посл}. \qquad (11)$$

Если для снижения угрозы может быть применено несколько мер, то следует построить модели воздействия по каждой из них. Далее следует исходить из того, что в случае одновременного принятия нескольких мер рискообразующий потенциал $q_l$ угрозы, к которой относятся все указанные меры, не может быть уменьшен ниже нуля.

Таким образом, если сумма потенциалов снижения риска по каждой из мер окажется больше оценки рискообразующего потенциала угрозы в данном событии риска

$$\sum_{n=1}^{N^d} \overline{q_l^n} > q_l,$$

то значения потенциалов мер должны быть нормированы таким образом, чтобы их сумма была равна рискообразующему потенциалу угрозы по указанному событию риска

$$\sum_{n=1}^{N^d} \overline{q_l^n}^{норм} = q_l, \qquad (12)$$

где $N^d$ – количество мер, принимаемых для снижения угрозы $y_l$.

Такого рода операции выполняются для всех событий риска, включающих угрозу, к которой относится данная мера, но только в том случае, если выполнение этих операций приведет к получению большего значения оценки потенциала меры.

Имеет смысл определить для данной меры $d_k$ множество $D_l^k$ нормированных значений ее рископонижающего потенциала по каждому из событий риска, в которые входит парируемая ею угроза $y_l$.

В качестве окончательного значения оценки потенциала меры защиты по данной угрозе принимается максимальное значение потенциала снижения риска данной меры, полученное при построении моделей воздействия этой меры защиты по каждому из событий риска, в которые входит угроза, парируемая данной

мерой

$$\overline{\overline{q_l^k}} = \max_{n=1}^{N^{O_l}} D_l^k . \qquad (13)$$

Всякая мера принимается по отношению к объекту, с которым связана угроза, ею парируемая. При этом может существовать целая совокупность угроз данному объекту, чей потенциал также может быть понижен указанной мерой. Таким образом, общий потенциал снижения риска меры защиты $d_k$ будет находиться как сумма рассчитанных оценок значимостей этой меры по всем угрозам, относимым к указанному объекту

$$\overline{q^k} = \sum_{n=1}^{N^{O_i}} \overline{\overline{q_n^k}} , \qquad (14)$$

где $\overline{\overline{q_n^k}}$ – частные рискообразующие потенциалы угроз $y_n \in Y^{O_i}$.

Однако если суммарный потенциал снижения рисков всех мер, относимых к данному объекту, превысит рискообразующий потенциал этого объекта

$$\sum_{n=1}^{N^D} \overline{q^n} > \omega^{O_i} ,$$

то должна быть выполнена процедура нормирования полученных значений потенциалов мер так, чтобы их общая сумма была равна рискообразующему потенциалу этого объекта

$$\sum_{n=1}^{N^D} \overline{q^n}^{\text{íîðì}} = \omega^{O_i} , \qquad (15)$$

где $N^D$ – количество мер, принимаемых для снижения рискообразующего потенциала объекта $\omega^{O_i}$.

Для окончательной оценки значимости меры $d_k$ необходимо также учесть стоимость ее осуществления $\overline{\Omega}_k$. Меры, для которых $\overline{q^k}^{норм} > \overline{\Omega}_k$, идентифицируются как значимые. При реализации стоимостного подхода сумма

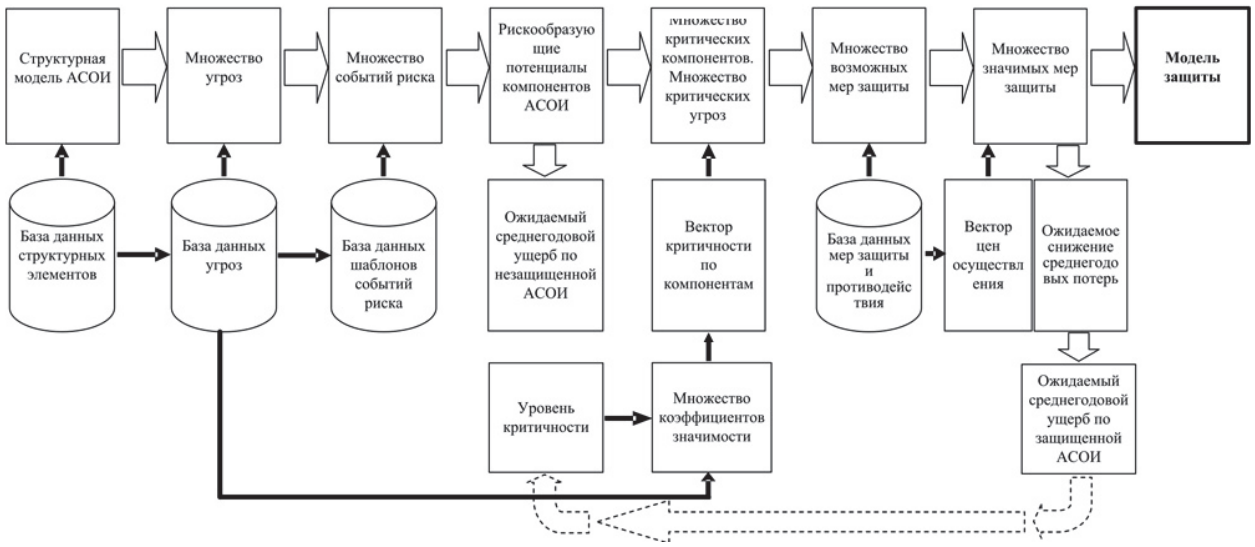
$$\sum_{n=1}^{N^{d_k}} (\overline{q^n}^{норм} - \overline{\Omega}_n) , \qquad (16)$$

где $N^{d_k}$ – количество значимых мер, определяющее ожидаемую величину снижения среднегодовых потерь для системы в оцениваемой конфигурации.

Если снижение среднегодовых потерь будет недостаточным и ожидаемые потери превзойдут уровень критичности, следует задать новое значение уровня критичности и повторить вычисления. В любом случае будет полезно экспериментально определить, изменяя с некоторым шагом уровень критичности, до какой величины он потенциально может быть снижен.

Таким образом, предложенные в развитие методологии анализа защищенности АСОИ,методы позволяют построить оптимальную модель ее защиты от внешних угроз.

Порядок применения методологии представлен на рисунке.




## Заключение

С каждым элементом системы и соответствующими ему угрозами можно связать некоторое множество возможных мер защиты и противодействия этим угрозам. Путем анализа того, как изменятся параметры событий риска в случае применения каждой из рассматриваемых мер, рассчитываются новые значения этих параметров. На основании данных оценок определяются частный и общий рископонижающие потенциалы возможных мер защиты, которые характеризуют величину снижения ожидаемых потерь в случае их применения. Множество значимых мер защиты образует оптимальную модель защиты АСОИ. Таким образом, предлагаются метод определения критических компонентов, представляющих угрозу безопасности в силу недостаточной защищенности автоматизированной системы обработки информации, а также метод определения значимых мер по предотвращению возникновения информационных рисков, основанный, в отличие от известных, на оценке рискообразующих потенциалов угроз и рископонижающих потенциалов мер защиты от этих угроз, и позволяющий в дополнение к методологии анализа защищенности АСОИ построить оптимальную модель ее защиты.

ЛИТЕРАТУРА

1. *Бурдин О.А.* Оценка рисков компьютеризации информационных систем // Проблемы управления информационной безопасностью. Сб. трудов Института системного анализа РАН. – М., 2002. – С.106-111.
2. *Бурдин О.А.* Система автоматизации управления информационной безопасностью больших организационных систем // Проблемы управления информационной безопасностью. Сб. трудов Института системного анализа РАН. – М., 2002. – С.164-217.
3. *Астахов А.* Анализ защищенности корпоративных систем // Открытые системы. – 2002. – № 7-8 (75-76). – С. 44-49.
4. *Петренко А. А.*, *Петренко С. А.* Метод оценивания информационных рисков организации // Проблемы управления информационной безопасностью. Сб. трудов Института системного анализа РАН. – М., 2002. – С.112-124.

*E-mail:*
*Сельвесюк Николай Иванович – selvesyuk@yandex.ru;*
*Островский Александр Сергеевич – aleksandr_ostrovsky@mail.ru;*
*Сливинский Василий Дмитриевич – maglee@mail.ru.*