УДК 681.324:681.326

РЕШЕНИЕ ЗАДАЧИ ВЫБОРА ОПТИМАЛЬНОГО ВАРИАНТА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ПОМОЩЬЮ МЕТОДА ЭКСПЕРТНОГО ОЦЕНИВАНИЯ

Т. В. Молдованин,
аспирант
Российский университет дружбы народов

Рассмотрен один из подходов к выбору оптимального варианта комплексной защиты информации на примере информационно-управляющей системы предприятия, основанный на экспертной оценке. Рассмотрены задачи оценки степени согласованности экспертных суждений и способы улучшения этой согласованности.

The problem of information complex security optimal variant selection by the example of information-controlling system of enterprise is given in this work. The group expertise is used for reliability support of evaluation results. Problems of dimension of agreement evaluation of expert evaluations and improvement of this agreement are also given in this work.

Введение

Основной характеристикой информационно-управляющей системы (ИУС) предприятия является ежедневное обеспечение сотрудников необходимым и достаточным для выполнения служебных обязанностей информационным сервисом. Число ежедневно обрабатываемой информации, гибкость технологии и скорость ее аналитической обработки требуют активного взаимодействия и высочайшего уровня надежности, а также квалифицированно построенной системы защиты. Задача усложняется сложностью структуры, которая является территориально-распределенной за счет наличия отдаленных площадок.

Описание ИУС предприятия

Рассматривается задача выбора оптимального варианта комплексной защиты информации информационно-управляющей системы конкретного предприятия. ИУС предприятия представляет собой сложный взаимоувязанный комплекс средств, призванный решать задачи оперативного управления технологическими процессами и процессами учета (рисунок). Среда передачи данных (Ethernet и Internet) является одним из ключевых звеньев при анализе степени защищенности ИУС. Использование технологий передачи данных просто невозможно без обеспечения надежной сетевой защиты каждого компьютера в отдельности.

При этом трудно достигнуть гарантий безопасности только путем шифрования отдельных видов трафика или использования только межсетевых экранов и систем обнаружения атак, устанавливаемых на границах сетей. Единственным способом, позволяющим обеспечить высокий уровень безопасности работы компьютеров в сети в этих условиях, является реализация максимального уровня контроля над всем трафиком, поступающим в компьютер извне, и его шифрование при соединениях с другими компьютерами.

Анализ степени защищенности ИУС предприятия

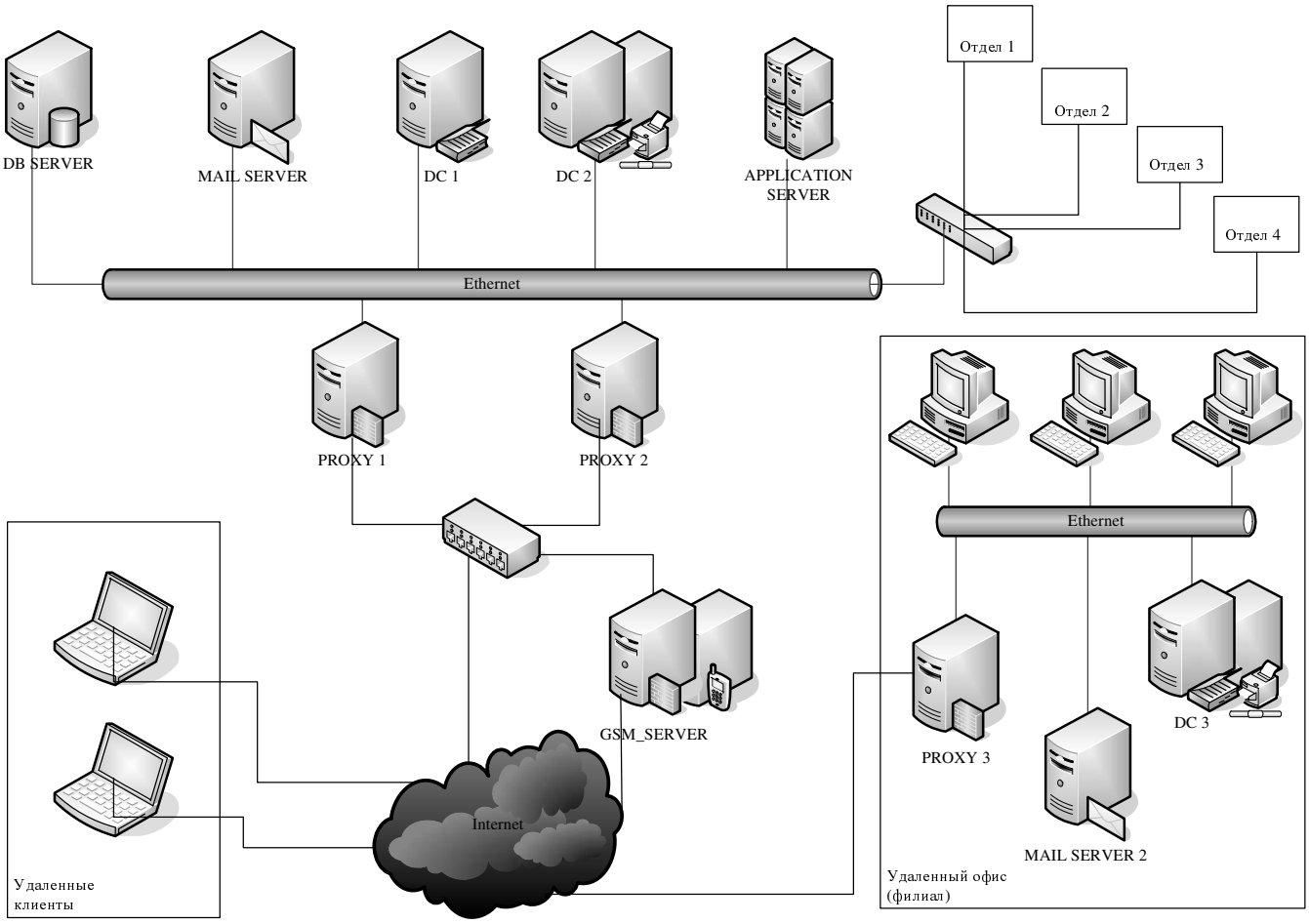
Анализ степени защищенности ИУС предприятия осуществлялся сотрудниками информационного отдела, выступающими в качестве экспертов, которым предложили оценить методом ранжирования следующие угрозы информационной безопасности.

1. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных, и т. п.).

2. Неправомерное отключение оборудования или изменение режимов работы устройств и программ.

3. Неумышленная порча носителей информации.

4. Запуск технологических программ, способных при некомпетентном использовании вызвать



■ *Схема ИУС предприятия*

потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения (форматирование или реструктуризацию носителей информации, удаление данных и т. п.).

5. Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях).

6. Заражение компьютера вирусами.

7. Неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной.

8. Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. д.).

9. Проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации.

10. Игнорирование организационных ограничений (установленных правил) при работе в системе.

11. Вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т. п.).

12. Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности.

13. Пересылка данных по ошибочному адресу абонента (устройства).

14. Ввод ошибочных данных.

15. Неумышленное повреждение каналов связи.

16. Физическое разрушение системы (путем взрыва, поджога и др.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т. п.).

17. Отключение или вывод из строя подсистем обеспечения функционирования вычислительных

систем (электропитания, охлаждения и вентиляции, линий связи и т. д.).

18. Действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т. п.).

19. Внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность).

20. Вербовка (путем подкупа, шантажа и т. п.) персонала или отдельных пользователей, имеющих определенные полномочия.

21. Применение подслушивающих устройств, дистанционная фото- и видеосъемка и т. д.

22. Перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и др.).

23. Перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему.

24. Хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ).

25. Несанкционированное копирование носителей информации.

26. Хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.).

27. Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.

28. Чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, воспользовавшись недостатками мультизадачных операционных систем и систем программирования.

29. Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т. д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»).

30. Несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.

31. Вскрытие шифров криптозащиты информации.

32. Внедрение аппаратных спецвложений, программных «закладок» и «вирусов» («троянских коней» и «жучков»), т. е. таких участков программ, которые не нужны для осуществления заявленных функций, но позволяют преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы.

Для определения наибольшей угрозы вычислялось среднее значение $\tilde{x}_i$ места i-угрозы, σ_i^2 — среднеквадратичное отклонение i-угрозы от ее среднего значения $\tilde{x}_i$ по формулам[1]:

$$\tilde{x}_i = \frac{1}{m}\sum_{j=1}^{m} c_{ij},$$

$$\sigma_i^2 = \frac{1}{(m-1)}\sum_{j=1}^{m}(c_{ij} - \tilde{x}_i)^2.$$

По всем i-угрозам выставлены предварительные ранги r. Все данные сведены в табл. 1.

Для повторного ранжирования вычислялись коэффициенты компетентности экспертов

$$\alpha_j = \frac{\frac{1}{D_j}}{\sum_{j=1}^{m}\frac{1}{D_j}}$$

на основе ранговой корреляции по формуле Спирмена

$$\rho_j = 1 - \frac{6}{n(n^2-1)} D_j,$$

где $D_j = \sum_{i=1}^{n} d_{ij}^2$, $d_{ij} = r_i - c_{ij}$.

С помощью коэффициентов ранговой корреляции повторно вычислялись среднее значение $\tilde{x}_i^*$ места i-угрозы и $\tilde{\sigma}_i^2$ — среднеквадратичное отклонение i-угрозы от ее среднего значения $\tilde{x}_i^*$:

$$\tilde{x}_i^* = \sum_{j=1}^{m}\alpha_j c_{ij},$$

$$(\sigma_i^*)^2 = \sum_{j=1}^{m}\alpha_i (c_{ij} - \tilde{x}_i^*)^2.$$

Формирование окончательных рангов (с учетом компетентности экспертов) проводилось по формуле

$$\gamma_i = \frac{\frac{1}{r_i^*}}{\sum_{i=1}^{n}\frac{1}{r_i^*}}.$$

Были получены весовые коэффициенты каждой угрозы (табл. 2).

[1] **Конеев И. Р.** Информационная безопасность предприятия. СПб.: БХВ Петербург, 2003. 733 с.

■ ***Таблица 1.*** *Первичное ранжирование*

Угроза	Эксперт					$\tilde{x}_i$	σ_i^2	r
	1	2	3	4	5			
1	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
2	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
3	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
4	7	8	7	7	7	7,20	0,20	8
5	7	8	7	7	7	7,20	0,20	8
6	27	27	27	27	27	27,00	0,00	27
7	11	11	11	11	11	11,00	0,00	11
8	7	4	7	7	7	6,40	1,80	4,5
9	2	2	2	2	2	2,00	0,00	2
10	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
11	7	5	7	7	7	6,60	0,80	4,5
12	7	8	7	7	7	7,20	0,20	8
13	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
14	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
15	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
16	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
17	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
18	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
19	27	27	27	27	27	27,00	0,00	27
20	27	27	27	27	27	27,00	0,00	27
21	27	27	27	27	27	27,00	0,00	27
22	27	27	27	27	27	27,00	0,00	27
23	3	3	3	3	3	3,00	0,00	3
24	27	27	27	27	27	27,00	0,00	27
25	27	27	27	27	27	27,00	0,00	27
26	27	27	27	27	27	27,00	0,00	27
27	27	27	27	27	27	27,00	0,00	27
28	27	27	27	27	27	27,00	0,00	27
29	7	8	7	7	7	7,20	0,20	8
30	7	8	7	7	7	7,20	0,20	8
31	1	1	1	1	1	1,00	0,00	1
32	27	27	27	27	27	27,00	0,00	27

■ *Таблица 2. Повторное ранжирование*

Угроза	$\tilde{x}_i^*$	$\tilde{x}_i^* + \tilde{\sigma}_i^2$	r	α
1	16,50	17,16	16,5	0,02
2	16,50	17,16	16,5	0,02
3	16,50	17,16	16,5	0,02
4	7,74	8,41	8	0,03
5	7,74	8,41	8	0,03
6	27,00	27,66	27	0,01
7	11,00	11,66	11	0,02
8	4,77	5,43	4	0,06
9	2,00	2,66	2	0,12
10	16,50	17,16	16,5	0,02
11	5,51	6,17	5	0,05
12	7,74	8,41	8	0,03
13	16,50	17,16	16,5	0,02
14	16,50	17,16	16,5	0,02
15	16,50	17,16	16,5	0,02
16	16,50	17,16	16,5	0,02
17	16,50	17,16	16,5	0,02
18	16,50	17,16	16,5	0,02
19	27,00	27,66	27	0,01
20	27,00	27,66	27	0,01
21	27,00	27,66	27	0,01
22	27,00	27,66	27	0,01
23	3,00	3,66	3	0,8
24	27,00	27,66	27	0,01
25	27,00	27,66	27	0,01
26	27,00	27,66	27	0,01
27	27,00	27,66	27	0,01
28	27,00	27,66	27	0,01
29	7,74	8,41	8	0,03
30	7,74	8,41	8	0,03
31	1,00	1,66	1	0,25
32	27,00	27,66	27	0,01

Алгоритм расчета индекса согласованности в задачах группового выбора и принятия решений и улучшение согласованности суждений в нечетком экспертном оценивании

Одной из важнейших задач принятия решений является выбор множества наилучших объектов (критериев) из заданной совокупности с помощью экспертов. Для обеспечения надежности результатов оценивания обычно используется групповая экспертиза. В этом случае возникают задачи оценки степени согласованности экспертных суждений и улучшения этой согласованности.

В работе предлагается новый конструктивный алгоритм вычисления индекса согласованности, основным отличием которого от известных подходов является простота математической формулировки и использование при вычислениях стандартных линейно-алгебраических операций. Разложение матрицы ранговых экспертных оценок **A** размером $n \times m$ $(n \le m)$ по сингулярным числам определяется соотношениями

$$\mathbf{A} = \cup \sum \mathbf{V}^T,\ \mathbf{U}^{-1} = \mathbf{U}^T,\ \mathbf{V}^{-1} = \mathbf{V}^T. \qquad (1)$$

Уравнение $\mathbf{A} = \cup \sum \mathbf{V}^T$ можно переписать в виде

$$\mathbf{A} = \boldsymbol{\sigma}_1 \mathbf{P}_1 + \boldsymbol{\sigma}_2 \mathbf{P}_2 + \ldots + \boldsymbol{\sigma}_n \mathbf{P}_n, \qquad (2)$$

где $\mathbf{P}_i = \mathbf{u}_i \mathbf{v}_i^T$ — матрица ранга 1 — есть внешнее произведение столбца матрицы **U** и соответствующего столбца матрицы **V**.

Предлагается в качестве индекса согласованности экспертных суждений использовать соотношение

$$\mathbf{IC} = \|\boldsymbol{\sigma}_1 \mathbf{P}_1\|_2 / \|\mathbf{A}\|_2 = \boldsymbol{\sigma}_1^2 / \sum \boldsymbol{\sigma}_1^2, \qquad (3)$$

причем если **A** — согласованная матрица ранговых экспертных оценок, то при этом ранг матрицы **A** равен 1, $\mathbf{A} = \mathbf{u}_1 \boldsymbol{\sigma}_1 \mathbf{v}_1^T$ и $\mathbf{IC} = 1$, а для несогласованных матриц $\mathbf{IC} < 1$.

Ввиду большой трудоемкости нахождения индекса согласованности по соотношению (1) с использованием разложения матрицы **A** по сингулярным числам разработан эффективный итерационный алгоритм, позволяющий на порядок уменьшить вычислительные затраты. Особенности данного алгоритма:

- находятся наибольшие сингулярные числа и соответствующие им правые и левые сингулярные векторы (сингулярные тройки) с использованием модификации степенного метода для собственных значений симметричной матрицы;
- поочередно, начиная с первого, находятся слагаемые соотношения (2), при этом производится последовательное уменьшение ранга матрицы, получаемой как разность между **A** и суммой найденных членов ряда для **A**;

• на каждом шаге выполняется ортогонализация рассчитанных сингулярных векторов к ранее найденным сингулярным подпространствам;

• используются 2 критерия окончания вычислительного процесса (нахождение первых k сингулярных троек и/или достижение заданной степени аппроксимации исходной матрицы).

Предлагаемый алгоритм является конструктивным в том смысле, что в результате вычислений, кроме индекса согласованности, находятся и векторы ранжирования альтернатив и критериев, в качестве которых используются нормализованные сингулярные векторы $\mathbf{v}_1$ и $\mathbf{u}_1$ соответственно.

Для улучшения согласованности суждений в нечетком экспертном оценивании предлагается итерационный алгоритм, включающий следующие шаги (этапы):

1) нахождение по соотношениям (1) и (2) наилучшей аппроксимации матрицы **A** матрицей ранга 1 в смысле метода наименьших квадратов, являющейся согласованной матрицей экспертных суждений (МЭС);

2) расчет среднего отклонения элементов исходной матрицы **A** от найденной ближайшей согласованной МЭС;

3) отнесение к достоверным суждения исходной МЭС, величина которых превышает величину среднего отклонения, и замену недостоверных суждений в матрице **A** оценками равной важности;

4) повторное выполнение этапов 1–3 до достижения заданной величины индекса согласованности МЭС.

Заключение

В результате экспертизы анализа степени защищенности ИУС предприятия выделены следующие угрозы, которые имеют весовой коэффициент $\alpha \geq 0,7$:

– вскрытие шифров криптозащиты информации;

– проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

– перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему.

Из данных анализа угроз, проведенного экспертами предприятия, следует, что первостепенной задачей эффективного построения системы защиты информации является выбор метода шифрования.