КОМПЛЕКСНЫЕ ВОПРОСЫ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БИТ

А. Л. Антипов, А. И. Труфанов
Иркутский государственный технический университет

ГРАФ-МОДЕЛЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ

Данная работа посвящена структурным исследованиям информационных систем (ИС) предприятий. Для анализа информационного взаимодействия в качестве основы использована граф-модель информационных операций. Предлагаемая модель может применяться для совершенствования методик оценки информационных систем, дающих точное и наглядное представление о возможных рисках и одновременно поставляющих информацию о самой организации и состоянии ИС.

Задачи оптимизации информационно-вычислительных систем с учетом фактора риска и поиски их решений актуальны в настоящее время как никогда ранее. Для создания методологии оптимального построения систем весьма полезными нам представляются исследования информационного взаимодействия в условиях возможности возникновения угроз.

В предлагаемой работе для анализа информационного взаимодействия в качестве основы была использована граф-модель информационных операций, изложенная в работе [1]. В такой модели описание предприятия должно содержать:

— перечень и структуру всех значимых элементов;

— взаимные связи между элементами;

— характер этих взаимосвязей.

При описании информационной системы предприятия выделим два непересекающихся множества, так что элементы одного из них по определенному закону связаны между собой элементами другого, — множество информационных узлов и множество угроз. Кроме того, определим множество информационных потоков, которое не пересекается ни с множеством информационных узлов, ни с множеством угроз, но элементы которого взаимодействуют как с элементами множества информационных узлов, так и с элементами множества информационных потоков.

Определим граф, для чего зададим множество вершин, ребер, а также предикат, устанавливающий взаимную инцидентцию элементов этих множеств.

Считается, что граф

$$\chi = \chi(\varphi,\gamma,\rho,) \qquad (1)$$

задан, если даны: непустое множество вершин (множество информационных узлов) $\varphi \neq 0$, не пересекающееся с ним множество ребер (множество угроз) $\gamma(\gamma \cap \varphi = 0)$ и предикат (инцидентор) δ. Примем, что ξ — это тип информа-ционного потока. Для наглядности на графе каждому типу информационного потока присваивается цветовая маркировка. Аналитически предикат описывается логическим высказыванием следующего вида:

$$\rho = \rho(\varphi_i, \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{km}\psi_k)\varpi_\xi), \varphi_j), \quad (2)$$

которое означает, что при $\xi=1$ от $k=1$ до k ребер угроз γ_{km} одного типа информационного потока соединяет вершины φ_i и φ_j. Причем каждая угроза имеет свой рассчитанный вес — ψ. Для подсчета общего количества ребер между вершинами φ_i и φ_j необходимо просуммировать по ξ все ребра угроз с учетом веса каждого участвующего информационного потока ϖ.

Для наглядности описания целесообразно информационные узлы располагать таким образом, чтобы в начертании графа число пересечений различных ребер было минимально.

Для графа (1) для всякого элемента $\gamma_{km} \in A$ справедливо одно и только одно из следующих высказываний:

$$\exists\varphi_i\varphi_j\left[\varphi_i \neq \varphi_j \;\&\; \rho(\varphi_i, \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{km}\psi_k)\varpi_\xi), \varphi_j) \;\&\; \overline{\rho}(\varphi_j, \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{km}\psi_k)\varpi_\xi), \varphi_i)\right]; \quad (3)$$

$$\exists\varphi_i\left[\rho(\varphi_i, \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{km}\psi_k)\varpi_\xi), \varphi_i)\right]; \quad (4)$$

$$\exists\varphi_i\varphi_j\left[\varphi_i \neq \varphi_j \;\&\; \rho(\varphi_i, \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{km}\psi_k)\varpi_\xi), \varphi_j) \;\&\; \rho(\varphi_j, \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{km}\psi_k)\varpi_\xi), \varphi_i)\right]. \quad (5)$$

Логические высказывания (3)—(5) позволяют классифицировать ребра на ориентированные (направленные) ребра — дуги (3), петли (4) и неориентированные (ненаправленные) ребра — звенья (5). В модели звенья изображаются в виде совокупности двух (слитых в одну) двунаправленных дуг:

$$\widetilde{\rho}(\varphi_i, \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{km}\psi_k)\varpi_\xi), \varphi_j) \Leftrightarrow$$
$$\rho(\varphi_i, \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{km}\psi_k)\varpi_\xi), \varphi_j) \vee \rho(\varphi_j, \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{km}\psi_k)\varpi_\xi), \varphi_i). \quad (6)$$

На рис. 1 представлен граф информационного взаимодействия и угроз в рамках предприятия (количество угроз и типов информационных потоков выбрано для примера произвольно).

Для более полного описания графа в модель включены элементы: информационный вес узла, путь и контур.

Пусть информационный вес объекта — $C_i = \sum_{\xi=1}^{\xi}((\prod_{k=1}^{k}\gamma_{ki}\psi_k)\varpi_\xi)$. (7)

Путем $P_{0,N}$ из вершины в вершину для одного типа информационного потока с учетом его веса будет следующая конечная цепь:

$$\varphi_0(\prod_{k=1}^{k}\gamma_{k1}\psi_k)\varpi_\xi\varphi_1(\prod_{k=1}^{k}\gamma_{k2}\psi_k)\varpi_\xi\varphi_2..\varphi_{N-1}(\prod_{k=1}^{k}\gamma_{kN}\psi_k)\varpi_\xi\varphi_N,$$

для которой истинно высказывание: $\&_{i=0}^{N-1}\rho(\varphi_i, (\prod_{k=1}^{k}\gamma_{k\,i+1}\psi_k)\varpi_\xi, \varphi_{i+1})$.

В качестве количественных характеристик пути P используются: длина пути $l(P)$ и вес пути $\Omega(P)$. Число ребер, образующих путь, — длина пути. Длина пути $l(P_{0,N}) = N$.

Вес пути вычисляется в два этапа:

- Вычисление весов информационных ребер, связывающих смежные объекты.
  - Произведение ребер угроз одного типа информации с учетом их веса;
  - Суммирования ребер всех типов информации, связывающих смежные объекты с учетом весов информационных потоков.
- Произведение весов информационных ребер на всем протяжении пути.

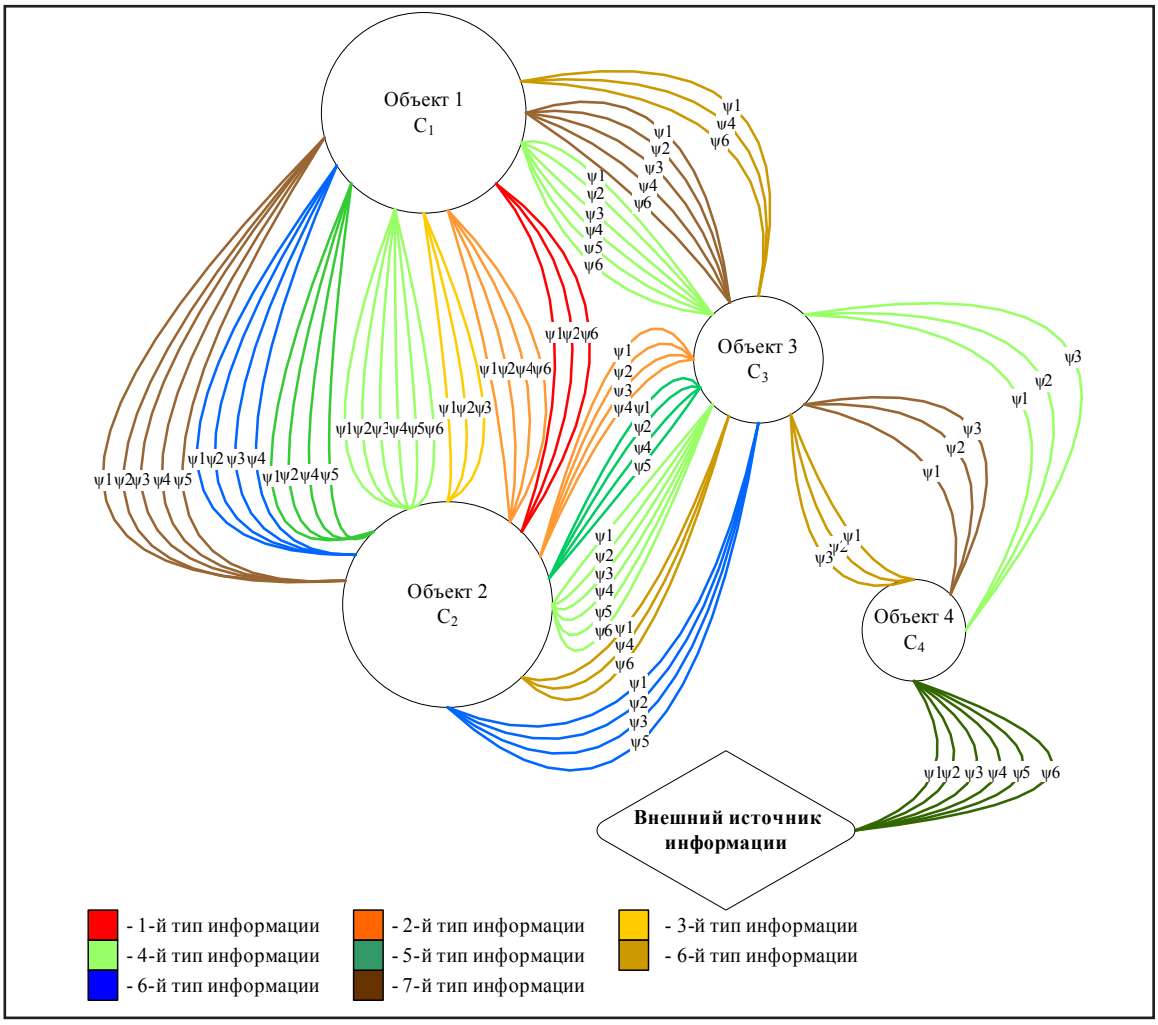

Рис. 1. Граф-модель информационных ресурсов предприятия

Т. е. вес пути: $\Omega(P_{0,N}) = \prod_{i=1}^{N} \Omega(\prod_{k=1}^{k} \gamma_{ki} \psi_k) \varpi_\xi)$. (10)

Для упрощения работы с моделью в ней используются только простые элементарные пути (пути, в которых ни одна из вершин не встречается дважды).

При выборочном по объектам исследовании предприятия строится подграф предприятия.

По мере разрешения вопросов с отдельными угрозами (нейтрализация угроз) проводится перерисовка графа, т. е. строится суграф. Суграфом называется часть графа, имеющая то же множество вершин, что и сам граф. При сохранении множества вершин исходного графа, но при полном исключении всех ребер (абсолютная защита информационной системы предприятия) строится пустой суграф предприятия.

Настоящая топологическая модель может быть эффективно использована при структурном синтезе информационной системы предприятия, отдельных ее компонентов и процессов взаимодействия информационной системы предприятия и системы информационной безопасности.

Достоинства настоящей модели заключаются в следующем:

• использование настоящей модели в практической деятельности позволяет оптимизировать структуру информационной системы предприятия;

• модель наглядно отображает процессы информационного обмена между подразделениями предприятия и взаимообмен информационными ресурсами с внешними контрагентами: вершины графа взаимнооднозначно соответствуют информационным узлам, а дуги — исследуемым процессам;

• в рамках модели также визуально отображаются вероятные угрозы;

• модель в виде графа позволяет эффектно и эффективно продемонстрировать механизмы действия прямых и обратных связей системы, дифференцировать потоки информации, виды угроз и определить передачи между отдельными ее компонентами на этапе анализа;

• математический аппарат модели предоставляет методологию поиска ошибок в информационной системе.

На сегодняшний день существуют две основные методики оценки рисков информационной безопасности: метод оценки рисков, основанный на построении модели угроз и уязвимостей, и метод оценки рисков, основанный на построении модели информационных потоков. По нашему мнению, возникла необходимость проработки новой методики оценки рисков, учитывающей как модель угроз, так и модель информационных потоков. Предлагаемая граф-модель может быть использована в качестве базиса подобной методики.

СПИСОК ЛИТЕРАТУРЫ:

1. *Остапенко Г. А.* Информационные операции и атаки в социотехнических системах. Учебное пособие для вузов / Под ред. чл.корр. РАН В. И. Бори-сова. М.: Горячая линия — Телеком, 2007. — 134 с.