УДК 004.8

ОБ ОДНОМ ПОДХОДЕ К ОРГАНИЗАЦИИ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЛОЖНОЙ СЕТИ

Е.В. Аникина
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: ajanet@ipu.ru

А.О. Калашников
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: aokalash@ipu.ru

Ключевые слова: сложная сеть, мониторинг информационной безопасности, сенсор безопасности, распределение ресурса, двудольный граф.

Аннотация: В работе рассматривается один из методов эффективного распределения ограниченного ресурса специализированных устройств (сенсоров) для мониторинга информационной безопасности узлов сложной сети.

1. Введение

Приоритетной целью государственной политики на современном этапе является ускоренный переход к цифровой экономике. Данный переход характеризуется интенсивным внедрением и использованием информационных технологий в сферах экономики и финансов, промышленности и энергетики, транспорта и связи, государственного и муниципального управления, обороны и безопасности, науки и культуры, образования и здравоохранения, и многих других. Однако, широкое использование информационных технологий немыслимо без повышенного внимания к проблемам их безопасности. И в первую очередь это относится к вопросам обеспечения информационной безопасности объектов *критической информационной инфраструктуры Российской Федерации* (далее – КИИ РФ) и КИИ РФ в целом. О том, что важность указанной проблемы отчетливо осознается, в том числе, на уровне Президента и Правительства Российской Федерации, говорит и недавно вступивший в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1].

В соответствии с [1] (статья 7) *категорирование* объекта КИИ РФ представляет собой установление соответствия объекта КИИ РФ критериям значимости, присвоение ему одной из категорий значимости и проверку сведений о результатах ее присвоения.

Категорирование объектов КИИ РФ осуществляется исходя из:

- *социальной значимости*, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной

инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

- *политической значимости*, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;
- *экономической значимости*, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам КИИ РФ и (или) бюджетам Российской Федерации;
- *экологической значимости*, выражающейся в оценке уровня воздействия на окружающую среду;
- значимости объекта КИИ РФ для *обеспечения обороны страны, безопасности государства и правопорядка*.

При этом устанавливаются три категории значимости объектов критической информационной инфраструктуры – первая, вторая и третья.

Для успешной реализации мероприятий по обеспечению безопасности объектов КИИ РФ и КИИ РФ в целом необходимо решение целого ряда сложных научно-технических задач, из которых задача мониторинга информационной безопасности КИИ РФ, в том числе, с помощью специализированных устройств, является одной из ключевых.

Именно решению задачи эффективного распределения ограниченного ресурса специализированных устройств (сенсоров безопасности) для мониторинга информационной безопасности узлов гетерогенной сети, такой, как КИИ РФ или Интернет и будет посвящено дальнейшее содержание настоящей работы.

Необходимо отметить, что впервые близкая по постановке задача была рассмотрена в [2] (подробный анализ и библиографию см. там же), где рассматривалась проблема распределения ограниченного ресурса компьютерной системы, представленного некоторым количеством различных устройств между множеством пользователей, принадлежащих различным классам. Ключевым отличием задачи, рассматриваемой в настоящей работе от задачи, представленной в [2], является переход от рассмотрения множества уникальных устройств к рассмотрению множества групп однотипных устройств, что представляет собой существенное обобщение и усложнение исходной задачи. Тем не менее, отдельные результаты, полученные в [2] будут использованы в данной работе.

Рассмотрим формальную постановку задачи.

Пусть имеется сложная сеть, состоящая из узлов, относящихся к различным классам $\mathcal{K} = \{1, \dots, K\}$. Примерами таких сетей могут служить совокупность сетей, представляющих собой элементы КИИ РФ или Интернет. Обозначим X_k – количество узлов сети, относящихся к классу $k \in \mathcal{K}$ и $X = \sum_{k=1}^{K} X_k$ – общее количество узлов сети.

Положим, далее, что имеется некоторое количество специализированных устройств – сенсоров для мониторинга информационной безопасности узлов сети (далее – сенсор безопасности), также относящихся к различным классам $\mathcal{M} = \{1, \dots, M\}$. Обозначим Y_m – количество сенсоров безопасности, относящихся к классу $m \in \mathcal{M}$ и $Y = \sum_{m=1}^{M} Y_m$ – общее количество сенсоров. Будем полагать, что сенсоры безопасности различных классов обладают, в общем случае, различной эффективностью мониторинга информационной безопасности в отношении узлов сети, также относящихся к различным классам.

В качестве сенсоров безопасности могут выступать не только специализированные устройства, но и программные агенты и даже эксперты и аудиторы информационной безопасности. Но, в рамках данной работы мы, будем предполагать, что сенсорами безопасности будут являться именно специализированные устройства для мониторинга состояния узлов сети.

Будем считать, что эффективность (полезность) сенсора безопасности класса $m \in \mathcal{M}$ является функцией от числа узлов, мониторинг которых осуществляет указанный сенсор: $\sigma_m(x)$, $m \in \mathcal{M}$, $x \in \mathbb{N}_0 = \{0, 1, 2, \dots\}$. В рамках данной работы, для простоты, будем полагать, что $\sigma_m(x)$ – вогнутая функция, которая не зависит от конкретных классов узлов, а определяется только общим числом узлов сети, мониторинг которых осуществляет данный сенсор.

Обозначим $N_{m,k} \geq 0$ – максимальное число узлов класса $k \in \mathcal{K}$, которое может промониторить сенсор безопасности класса $m \in \mathcal{M}$ и $N_m \geq 0$ – суммарное максимальное число узлов, которое может промониторить сенсор безопасности класса $m \in \mathcal{M}$. Данное ограничение является вполне естественным, поскольку, с одной стороны, за конечный период времени любой сенсор безопасности может проверить только ограниченное число узлов, а с другой, например, может оказаться, что сенсор безопасности класса $m \in \mathcal{M}$ не может быть использован для мониторинга узлов класса $k \in \mathcal{K}$.

Таким образом, наша задача заключается в нахождении такого распределения узлов сети по сенсорам безопасности, которое максимизирует суммарную эффективность (полезность) всех устройств пока удовлетворяются вышеприведенные ограничения.

Пусть $x_{m,k}^i$ – число узлов класса $k \in \mathcal{K}$, мониторинг которых осуществляет *i*-й сенсор класса $m \in \mathcal{M}$, $i \in \{1, 2, \dots, Y_m\}$. Обозначим $x_m^i = \sum_{k=1}^{K} x_{m,k}^i$ – суммарное число узлов различных классов, мониторинг которых осуществляет *i*-й сенсор класса $m \in \mathcal{M}$, $x_m = \sum_{i=1}^{Y_m} x_m^i$ – суммарное число узлов различных классов, мониторинг которых осуществляются сенсорами класса $m \in \mathcal{M}$ и $z_k = \sum_{m=1}^{M} \sum_{i=1}^{Y_m} x_{m,k}^i$ – суммарное число узлов класса $k \in \mathcal{K}$, мониторинг которых осуществляется сенсорами всех классов.

Тогда наша задача может быть формально записана следующим образом:

(Task) $\sum_{m=1}^{M} \sum_{i=1}^{Y_m} \sigma_m(x_{m,k}^i) \rightarrow max$

при следующих ограничениях:

$$x_{m,k}^i \in \{0,1, \dots, N_{m,k}\}, x_m^i \leq N_m, z_k = X_k, k \in \mathcal{K}, m \in \mathcal{M}, i \in \{1, 2, \dots, Y_m\}.$$

При решении данной задачи в [3] был разработан и представлен базовый алгоритм на основе построения допустимого двудольного графа $G(\bar{X})$, реализующего все потенциальные распределения каждого узла сети по сенсорам безопасности и допустимых назначений $\bar{X} = [x_{m,k}^i], T(\bar{X}, L), \bar{X}(j-1) = [x_{m,k}^i(j-1)]$.

Общий алгоритм решения задачи Task, приведенный в [3], представляет собой последовательное решение задач Task (j) , при $j = 1, 2, \dots, X$, использующих базовый алгоритм [3]. Доказательство корректности работы алгоритма, а также основного результата настоящей статьи, являющегося обобщением Теоремы 1 из [2] представлено в [3].

2. Оценка вычислительной сложности алгоритма

В работе [2] приводится оценка вычислительной сложности алгоритма, решающего задачу нахождения распределения ограниченного ресурса компьютерной системы, представленного некоторым количеством различных устройств между множеством пользователей, принадлежащих различным классам и имеющая вид:

$$O\ (M(LM + M^2 + LK)),$$

где *M* – число устройств, *L* – число пользователей и *K* – число классов пользователей.

Ключевым отличием задачи, рассматриваемой в данной работе, как уже было сказано выше, является переход от рассмотрения множества единичных устройств к рассмотрению множества групп однотипных устройств, что представляет собой существенное обобщение и усложнение исходной задачи. Тем не менее, поскольку, как и в [2]

решение задачи Task представляет собой последовательное решение задач Task (j), при $j = 1, 2, \dots, X$, то и в этом случае вычислительная сложность алгоритма решения задачи Task будет иметь вид:

$$O\ (Y(XY + Y^2 + XK)),$$

где Y – общее число сенсоров безопасности, X – общее число узлов сети и K – число классов узлов.

3. Заключение

В работе была рассмотрена задача нахождения такого распределения узлов сложной сети, относящихся к разным классам, по сенсорам безопасности, также относящихся к разным классам, которое бы максимизировало суммарную эффективность (полезность) функционирования всех сенсоров с учетом определенных для них ограничений. Был предложен общий алгоритм решения указанной задачи, доказана его корректность и проведена оценка его вычислительной сложности.

Необходимо отметить, что предложенный в данной работе метод эффективного распределения средств мониторинга информационной безопасности в рамках сложной сети может быть успешно использован в рамках решения других задач. Например, при оценке безопасности КИИ РФ, в том числе, на основе метода вейвлет-анализа [4] или управления информационной безопасностью КИИ РФ на основе выявления ее аномальных состояний с использованием механизмов комплексной оценки [5] и кластерного анализа [6, 7].

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Tantawi A.N., Towsley G., Wolf J. Optimal allocation of multiple class resources in computer systems // ACM SIGMETRICS Performance Evaluation Review. 1988. Vol. 16, No. 1. P. 253-260.
3. Калашников А.О., Аникина Е.В. Метод эффективного распределения сканеров для мониторинга информационной безопасности узлов гетерогенной сети // Информация и безопасность. 2018. Т. 21. № 4. С. 455-464.
4. Калашников А.О., Сакрутина Е.А. Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа // Информация и безопасность. 2017.Т. 20, № 4 (4). С. 478-491.
5. Калашников А.О. Управление информационными рисками организационных систем: механизмы комплексного оценивания // Информация и безопасность. 2016. № 3.С. 315-322.
6. Калашников А.О., Аникина Е.В. Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления ее аномальных состояний (часть 1) // Информация и безопасность.2018. Т.21. № 2 (4).С. 145-154.
7. Калашников А.О., Аникина Е.В. Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления ее аномальных состояний (часть 2) // Информация и безопасность.2018.Т. 21. № 2 (4). С. 155-164.