§7 МОДЕЛИ И МЕТОДЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Коробейников А. Г. Пирожникова О. И.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ РАСЧЕТА ВЕРОЯТНОСТИ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ПРОНИКНОВЕНИЯ НА ОБЪЕКТ ИНФОРМАТИЗАЦИИ

Аннотация: *Согласно действующему госстандарту, понятие "безопасность объекта информатизации" объединяет защиту четырех типов – физическую, техническую, правовую и криптографическую. Отсюда следует, что это понятие является комплексным. Кроме того, в соответствии с нормативными документами, защитные мероприятия для обеспечения информационной безопасности подразделяют на организационные и технические. За выполнение таких функций как ограничение угроз, сдерживание, предотвращение, обнаружение, уведомления о различных событиях на объекте информатизации, мониторинг состояния объектов информатизации, исправление ошибок, восстановление активов системы и т.д. отвечают технические защитные мероприятияАнализ современного состояния методов и средств одной из важнейших составляющей комплексной системы информационной безопасности, такой как системы охранной сигнализации, показал, что эти системы необходимо непрерывно развивать, для того, что бы они соответствовали постоянно повышающимся требованиям к современной защите объектов информатизации. Отсюда следует, что разработка математических моделей расчета вероятностей несанкционированного физического проникновения на объект информатизации, входящих в состав комплексной системы информационной безопасности, является актуальной задачей. Для решения поставленной задачи в представленной статье были использованы методы защиты информации, методы теории графов и теории вероятности. Представленные результаты были получены при помощи системы компьютерной алгебры Maple. Научная новизна заключается в разработке:- на базе теории графов математической модели расчета вероятности несанкционированного физического проникновения на объект информатизации. Сама модель строится за три этапа на основе конкретных исходных данных;- методики оценки вероятности обнаруже-*

DOI: 10.7256/2305-6061.2014.2.12504

ния системой охранной сигнализации несанкционированного физического проникновения на объект информатизации.

Ключевые слова: *Неограф, Ациклический граф, Несанкционированное физическое проникновение, Технические мероприятия защиты, Защита объекта информатизации, Орграф, Матрица смежности, Матрица весов, Алгоритм Дейстры, Сложение вероятностей*

Анализ современного состояния методов и средств одной из важнейших составляющей комплексной системы информационной безопасности, такой как системы охранной сигнализации, показал, что эти системы необходимо непрерывно развивать, для того, что бы они соответствовали постоянно повышающимся требованиям к современной защите объектов информатизации. Отсюда следует, что разработка математических моделей расчета вероятностей несанкционированного физического проникновения на объект информатизации (ОИ), входящих в состав комплексной системы информационной безопасности, является актуальной задачей. Для решения поставленной задачи в представленной статье были использованы методы защиты информации, методы теории графов и теории вероятности. Представленные результаты были получены при помощи системы компьютерной алгебры Maple [1].

Математическая модель расчета вероятности несанкционированного физического проникновения на объект информатизации строится за несколько этапов.

Первый этап. Строится ММ ОИ в виде ациклического графа G_1. Назначаем матрицу смежности, которая показывает связь между ij – ым и kl – ым местом (под местом понимается комната, лестница, коридор и т.д.). Схематически маршрут в таком графе можно представить в виде Рис. 1. Определяется вершина j_d, куда хочет попасть злоумышленник. Вычисляются все потенциально опасные маршруты из заданных вершин в вершину j_d.

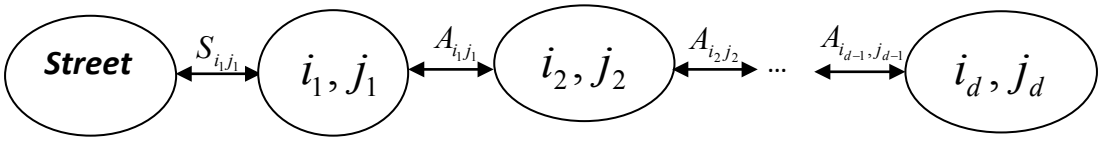

Рис.1. Маршрут с улицы в заданное место j_d

Для примера рассмотрим ОИ с тремя этажами и 5-ю местами на каждом этаже. За вершину 1 примем улицу. Первый этаж: 2,5 - служебные помещения, 3 - коридор, 4 - проходная, 6 – лестница. Второй этаж: 7,8,10 - служебные помещения, 9 – коридор, 11 – лестница. Третий этаж: 12,13,14 – служебные помещения, 15 – коридор, 16 – лестница. Зададим матрицу смежности $A_{смежн}$:

DOI: 10.7256/2305-6061.2014.2.12504

$$A_{смежн} = \begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}$$

Соответствующий граф представлен на рис. 2.

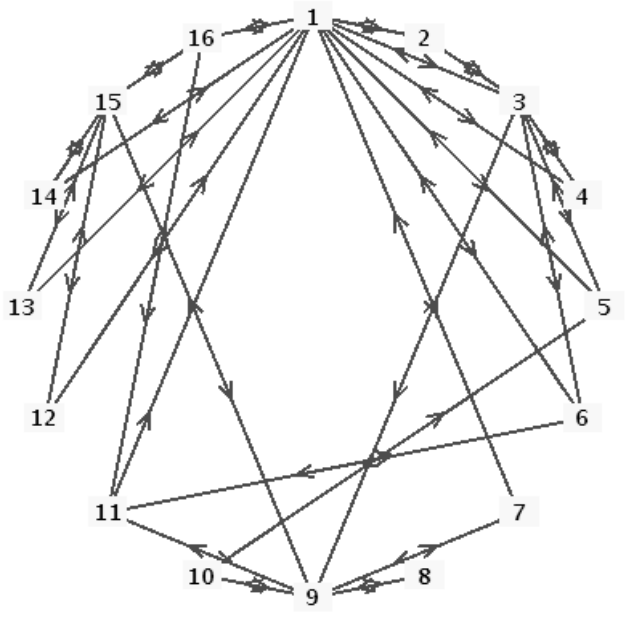

Рис.2. Неограф, соответствующий $A_{смежн}$

Предположим, что место, куда попытается проникнуть злоумышленник, соответствует

DOI: 10.7256/2305-6061.2014.2.12504

вершине 10. Вычисляются все потенциально опасные маршруты из заданных вершин в вершину под номером 10. В таблице 1 представлены результаты вычисления количества маршрутов из k – ой вершины в 10.

Таблица 1.

Длина/k	1	2	3	5	6	7	8	9	11	12	13	14	15	16
2	1	0	2	0	0	1	1	0	1	0	0	0	1	0
3	3	3	1	5	4	1	0	8	1	2	2	2	0	3
4	26	4	26	4	5	11	8	3	18	3	3	3	17	4
5	67	52	46	65	70	29	3	93	38	43	43	43	16	61

Второй этап. Задаем вес для каждого ребра, то есть задаем матрицу весов W. Веса выбираем из физических соображений. Используя матрицу W, преобразуем неограф G_1 во взвешенный орграф G_2. Далее, при помощи алгоритма Дейстры, вычисляем наиболее предпочтительные пути из заданных вершин в вершину j_d [2,3]. Продолжая пример, имеем матрицу W и список результатов вычисления наиболее предпочтительных путей с результирующими весами из заданных вершин в вершину 10.

[[1,4,3,6,11,9,10], 19], [[2,3,6,11,9,10], 17], [[3,6,11,9,10], 15], [[4,3,6,11,9,10], 17], [[5,3,6,11,9,10], 25], [[6,11,9,10], 14], [[7,9,10], 20], [[8,9,10], 20], [[9,10], 10], [[11,9,10], 12], [[12,15,16,11,9,10], 26], [[13,15,16,11,9,10], 26], [[14,15,16,11,9,10], 26], [[15,16,11,9,10], 16], [[16,11,9,10], 14].

$$W = \begin{pmatrix}
0 & 65 & 65 & 2 & 65 & 65 & 75 & \infty & \infty & \infty & 75 & 85 & 85 & 85 & 85 & 85 \\
65 & 0 & 2 & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty \\
65 & 10 & 0 & 2 & 10 & 1 & \infty & \infty & 200 & \infty & \infty & \infty & \infty & \infty & \infty & \infty \\
2 & \infty & 2 & 0 & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty \\
65 & \infty & 10 & \infty & 0 & \infty & \infty & \infty & \infty & 200 & \infty & \infty & \infty & \infty & \infty & \infty \\
65 & 0 & 1 & \infty & \infty & 0 & \infty & \infty & \infty & \infty & 2 & \infty & \infty & \infty & \infty & \infty \\
75 & 0 & \infty & \infty & \infty & \infty & 0 & \infty & 10 & \infty & \infty & \infty & \infty & \infty & \infty & \infty \\
\infty & 0 & \infty & \infty & \infty & \infty & \infty & 0 & 10 & \infty & \infty & \infty & \infty & \infty & \infty & \infty \\
\infty & 0 & 200 & \infty & \infty & \infty & 10 & 10 & 0 & 10 & 2 & \infty & \infty & \infty & 200 & \infty \\
\infty & 0 & \infty & \infty & 200 & \infty & \infty & \infty & 10 & 0 & \infty & \infty & \infty & \infty & \infty & \infty \\
75 & 0 & \infty & \infty & \infty & 2 & \infty & \infty & 2 & \infty & 0 & \infty & \infty & \infty & \infty & 2 \\
85 & 0 & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & 0 & \infty & \infty & 10 & \infty \\
85 & 0 & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & 0 & \infty & 10 & \infty \\
85 & 0 & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & 0 & 10 & \infty \\
85 & 0 & \infty & \infty & \infty & \infty & \infty & \infty & 200 & \infty & \infty & 10 & 10 & 10 & 0 & 2 \\
85 & 0 & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & 2 & \infty & \infty & \infty & 2 & 0
\end{pmatrix}$$

Третий этап. Базируясь на полученных результатах, устанавливаем в указанные места сенсоры определяющие физическое проникновение. Формально это означает, что рассчитанным вершинам приписывается вероятность обнаружения физического проникно

DOI: 10.7256/2305-6061.2014.2.12504

вения, соответствующая техническими характеристиками применяемых сенсоров, то есть задается вектор вероятностей обнаружения физического проникновения техническими средствами $ОФП_n=(p_1, p_2,..., p_n)$, где n – количество вершин в G_2. После этого, применяя теорему о сложении вероятностей, рассчитываются вероятности обнаружения физического проникновения на каждом из полученных путей.

Продолжая пример, имеем $ОФП_{16}=(p_1,..., p_{16})$. Зададим численные значения $ОФП_{16}$=(0.09,0.01,0.15,0.12,0.14,0.14,0.0,0.24, 0.3,0.75,0.34,0.5,0.5,0.55,0.3,0.34). Полученные результаты расчета вероятностей обнаружения физического проникновения на каждом из полученных путей представлены в таблице 2.

Таблица 2

Вероятности обнаружения физического проникновения

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
.932	.916	.915	.926	.927	.901	.825	.867	.825	.750	.884	.973	.973	.976	.947	.928

PP_1=0.9323880556, PP_2=0.916413805, PP_3=0.9155695, PP_4=0.92570116, PP_5 = 0.92738977, PP_6=0.90067, PP_7 = 0.825, PP_8 =0.867, PP_9=0.825, PP_{10}=0.75, PP_{11}=0.8845, PP_{12}=0.9733195, PP_{13}= 0.9733195, PP_{14}=0.97598755, PP_{15}=0.946639, PP_{16}= 0.92377

Обычно считается, что злоумышленнику известны значения матриц $A_{смежн}$ и W, а также вектора $ОФП_n$. Его цель в нахождении возможных путей, на которых его обнаружат с минимальной вероятностью. А вот цель комплексной системы защиты ОИ – сделать эту вероятность максимальной.

Библиография :

1. Коробейников А.Г., Гришенцев А.Ю. Разработка и исследование многомерных математических моделей с использованием систем компьютерной алгебры // СПбНИУ ИТМО.-Санкт-Петербург: СПбНИУ ИТМО, 2013.-100 с.
2. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оптимизация древовидной сети с резервированием коммутационных узлов и связей. //Телекоммуникации. 2013. № 2. – С. 42-48.
3. Гришенцев А.Ю., Коробейников А.Г. Постановка задачи оптимизации распределённых вычислительных систем // Программные системы и вычислительные методы.-2013.-4.-С. 370-375. DOI: 10.7256/2305-6061.2013.4.10548.

References:

1. Korobeinikov A.G., Grishentsev A.Yu. Razrabotka i issledovanie mnogomernykh matematicheskikh modelei s ispol'zovaniem sistem komp'yuternoi algebry // SPbNIU ITMO.-Sankt-Peterburg: SPbNIU ITMO, 2013.-100 s.

DOI: 10.7256/2305-6061.2014.2.12504

2. Bogatyrev V.A., Bogatyrev S.V., Bogatyrev A.V. Optimizatsiya drevovidnoi seti s rezervirovaniem kommutatsionnykh uzlov i svyazei. //Telekommunikatsii. 2013. № 2. – S. 42-48.
3. Grishentsev A.Yu., Korobeinikov A.G. Postanovka zadachi optimizatsii raspredelennykh vychislitel'nykh sistem // Programmnye sistemy i vychislitel'nye metody.-2013.-4.-C. 370-375. DOI: 10.7256/2305-6061.2013.4.10548.