УДК 681.322

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЫБОРА ОБОРУДОВАНИЯ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ НА ОСНОВЕ ПРИМЕНЕНИЯ ТЕОРИИ ИГР

С.Ю. ФЁДОРОВ, В.Н. ХАЛИЗЕВ

Кубанский государственный технологический университет,
350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
электронная почта: iitib@rambler.ru

В статье рассмотрены математическая модель выбора оптимального набора оборудования для интегрированной системы безопасности на основе применения методов теории игр. В настоящий момент в связи с ростом применения средств коммуникаций и вычислительной техники усиливается проблема обеспечения информационной безопасности. Проблема обеспечения безопасности всегда являлась очень важной. Для защиты от угроз современная концепция защиты информации предусматривает комплексный подход к её организации. Одними из основных являются методы и средства инженерно-технической защиты. Важнейшей составной частью инженерно-технических средств защиты информации являются технические средства охраны, которые образуют первый рубеж защиты компьютерных систем [1]. Сейчас одним из перспективных путей развития технические средства охраны является их объединение в единый комплекс – интегрированную систему безопасности (ИСБ). На рынке сегодня представлено огромное разнообразие технических средств охраны, и специалистам по информационной безопасности приходится принимать нелёгкие субъективные решения по выбору оборудования и могут быть ошибки. Поэтому использование модели на основе теории игр позволит обеспечить оптимизацию выбора технических средств охраны для защиты информации.

Ключевые слова: математическая модель выбора оптимального набора, интегрированные системы безопасности, теории игр, информационная безопасность.

Для поиска наиболее оптимальных стратегий защиты информационных ресурсов можно предложить математическую игру двух сторон, одной из которых является система защиты - ИСБ, а с другой - возможные действия нарушителей. В этом случае выигрыш злоумышленников будет равен проигрышу специалистов по информационной безопасности (ИБ) и можно получить матрицу для игры двух лиц с нулевой суммой. При этом строки $A_i(i=1,\ldots,n)$ некоторой матрицы будут приниматься в качестве стратегий нарушителей, а в качестве стратегий специалистов ИБ - её столбцы $B_j(j=1,\ldots, m)$. К стратегиям нарушителей можно отнести различные типовые сценарии (угрозы) действий нарушителей, которые могут привести к ущербу для предприятия (несанкционированное проникновение на объект, хищение

информации, теракт, пожар и т.д.), к стратегиям специалистов ИБ - различные технические средства охраны, предназначенные для защиты.

Таблица 1 - Таблица матричной игры

A_i / B_j		B_1	B_2	. . .	B_m
A_1	$p(x_1)$	a_{11}	a_{12}	. . .	a_{1m}
A_2	$p(x_2)$	a_{21}	a_{22}	. . .	a_{2m}
. . .	. . .	. . .	. . .	. . .	. . .
A_n	$p(x_n)$	a_{n1}	a_{n2}	. . .	a_{nm}

Анализ выбранного оборудования позволяет каждому техническому средству охраны сопоставить возможность и устранить определенные угрозы. Для проведения на компьютере игры надо также знать результаты игры при каждой паре стратегий A_i и B_j (например, a_{ij} - причинённый нарушителем материальный ущерб) и вероятности реализации сценария угрозы нарушителем $p(x_i)$ при выбранной стратегии x_i. Вероятности реализации угроз $p(x_i)$ берутся из сети Интернет, по результатам статистических исследований, используя на кафедре интегрированную систему безопасности «Интеллект». Если вероятности неизвестны, то можно предположить, что все они равновероятны, т. е. $p(x_i)=1/n$. В качестве коэффициентов a_{ij} матрицы игры рассматривать годовые потери для всех вариантов комбинаций $A_i(i= 1, \ldots,n)$ и $B_j(j=1,\ldots,m)$. Для этого сопоставить каждый типовой сценарий действий нарушителей с каждым методом защиты и определить ущерб, который может быть при этом нанесён. Покупка, установка и использование средств защиты требуют дополнительных затрат, что нужно вносить в ущерб при расчётах. Построив игровую матрицу (см. таблица 1) и проанализировав её, оцениваются затраты для каждого решения и выбираются наиболее эффективные варианты оборудования для всего диапазона сценариев действий нарушителей. Если построена такая игровая матрица, то наилучшей в условиях имеющейся информации будет стратегия системы защиты компьютерной информации B_j, при которой будут минимальны средние потери, т. е. будет минимальна сумма: $\sum_{i=1}^{n} a_{ij}p(x_i)$. Для выбора наиболее оптимального набора оборудования в качестве

стратегий используются различные сочетания сценариев действий нарушителей и видов оборудования. Прекращение использования или добавление нового средства можно рассматривать как переход от одной стратегии к другой. Поэтому разумное поведение игроков в матричной игре должно основываться на следующих рассуждениях.

Пусть нарушитель выбирает некоторую свою стратегию A_i. Тогда в наихудшем случае (в теории игр игроки предполагаются весьма осторожными и рассчитывают на наименее благоприятный поворот событий; такое положение дел для стратегий нарушителей может наступить, например, в случае, когда стратегия A_i станет известной специалисту ИБ) и он получит выигрыш $min\ a_{ij.}$ Поэтому нарушитель должен выбрать свою стратегию A_{i0} (см . формулу 1) так, чтобы максимизировать этот свой минимальный выигрыш :

$$\min_j a_{i0j} = \max_i \min_j a_{ij} \quad (1)$$

Значит, стоящий в правой части написанного равенства «максимин» является гарантированным выигрышем нарушителя. Аналогичные рассуждения, проводимые специалистом ИБ, показывают в формуле 2, что он должен выбирать такую свою стратегию B_{j0}, что

$$\min_i a_{ij0} = \min_j \max_i a_{ij} \quad (2)$$

Здесь стоящий справа «минимакс» является тем выигрышем нарушителя, больше которого он при правильных действиях специалиста ИБ получить не может. Поэтому фактический выигрыш нарушителя должен при разумных действиях специалистов ИБ лежать между правыми частями формул (1) и (2).

Расчет ущерба складывается из величин ущерба D_1, который может быть нанесён при реализации текущей стратегии нарушителем, если система не была защищена от неё техническими средствами охраны из текущей стратегии специалиста ИБ; и из общей стоимости D_2 всех технических средств охраны из текущей стратегии специалиста ИБ. Для подсчета общей стоимости нужных технических средств охраны D_2 сопоставляется текущий набор средств и все имеющиеся средства и суммируются величины стоимости тех средств, которые

присутствуют в первом наборе. Подсчет ущерба от реализации угроз D_1 вычисляется в два этапа. Сначала текущая стратегия злоумышленника сопоставляется с каждым из технических средств охраны из текущей стратегии специалиста ИБ, и если средство защищает от каких-то угроз из текущего набора, то данные угрозы удаляются из набора. Сопоставив текущий набор угроз со всеми средствами из текущей стратегии специалиста ИБ, получаем некоторое количество угроз, от которых система в данном случае не защищена. Полученные угрозы нужно сопоставить со всеми имеющимися угрозами и суммировать величины ущерба тех угроз, что присутствуют в полученном наборе. Далее эти две суммы D_1 и D_2 складываются и получается ущерб при применении текущей пары стратегий нарушителя и специалиста ИБ.

Для вычисления оптимальной стратегии необходимо в качестве основы для расчетов использовать формулу (2). Для начала составляется матрица, строками которой являются стратегии нарушителя, а столбцами - стратегии специалиста ИБ. На пересечении стратегий ставятся максимальные величины ущерба, рассчитанные по алгоритму. Таким образом, для каждой стратегии специалиста ИБ вычисляется максимально возможный ущерб. Теперь из всех полученных максимальных величин ущерба выбрать минимальное значение, т.е. $min\ max\ \{D_1+D_2\}$. Стратегия, соответствующая данному значению, и будет искомой *оптимальной стратегией [2]*.

Рекомендуется разработать программу, которая по введённым значениям стоимости оборудования и величины ущерба и в результате применения всех пар угроза-средство защиты вычисляет оптимальный набор из базы технических средств охраны. Результатом вычислений будет комплекс оптимального оборудования для интегрированной системы безопасности, общая стоимость оборудования и максимальный ущерб, который можно получить, при использовании данного комплекса. При выборе оборудования предпочтение отдаётся более дешёвым аналогам. В результате специалист ИБ может сначала получить оптимальный комплекс технических средств охраны, а потом изменять его исходя из величины максимального ущерба. В дальнейшем

при подготовки программы желательно применять веб-приложение с использованием HTML, CSS, языка JavaScript, JVM и с возможностью его запуска в браузере. Применение программного продукта и данной модели даст возможность специалисту ИБ выбрать наиболее оптимальный комплекс оборудования для построения на его основе интегрированной системы безопасности объекта информатизации.

ЛИТЕРАТУРА

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. Пособие для студ. высш. учеб. заведений / 2-е изд., стер. – М.: «Издательский центр академия», 2006. – 256 с.

2. Теория игр и защита компьютерных систем: учебное пособие / А.К. Гуц, Т.В. Вахний. - Омск: Изд-во ОмГУ, 2013. - 160 с.

REFERENCES

1. Horev P.B. Metody i sredstva zashhity informacii v komp'juternyh sistemah: ucheb. Posobie dlja stud. vyssh. ucheb. zavedenij / 2-e izd., ster. – M.: «Izdatel'skij centr akademija», 2006. – 256 s.

2. Teorija igr i zashhita komp'juternyh sistem: uchebnoe posobie / A.K. Guc, T.V. Vahnij. - Omsk: Izd-vo OmGU, 2013. - 160 s.

MATHEMATICAL MODEL OF SELECTING OF EQUIPMENT INTEGRATED SECURITY SYSTEMS BASED ON THE APPLICATION OF THE THEORY OF GAMES

S.YU. FEDOROV, V.N. KHALIZEV

Kuban State Technological University,
2, Moskovskaya st., Krasnodar, Russian Federation, 350072,
e-mail: iitib@rambler.ru

In the article the mathematical model of selecting the optimal set of equipment for integrated security systems, based of game theory. At present, the widespread use of means of communication and computer technology improves information security problems. Security problem has always been very important. In the article the mathematical model of selecting the optimal set of equipment, on the basis of the analysis of the security threats in order to choose the best solution for the synthesis of integrated security systems. Thus, the development of a mathematical model of selecting the optimal set of equipment for integrated security systems, based on the use of gaming techniques as relevant as ever.

Key words: mathematical model of selecting the optimal set, integrated security systems, theory of games, information security.