УДК 681. 3. 093

***В.А. Михеев, В. Г. Семин***

# Принципы и методы реализации политики безопасности системы обеспечения электромагнитной безопасности многофункциональных информационных сетей

*В статье приведены результаты разработки методов реализации политики безопасности, основанной на модели системы с зонной структурой организации системы обеспечения электромагнитной безопасности МИС ИС с учетом существующей концепции кластеризации систем технической защиты телекоммуникаций от электромагнитных воздействий.*

**Ключевые слова: обеспечение; модель; политика безопасности; конфликт: оптимальность; выбор**

Принципы реализации политики безопасности

Основной принцип реализации политики безопасности заключается в том, что любая реализация политики безопасности МИС ИС должна основываться на определенной формальной модели безопасности. В процессе реализации политики безопасности, в зависимости от особенностей системы и применяемого подхода, могут быть использованы различные модели. Рассмотрим наиболее общую модель, учитывающую стоимостной аспект создания системы обеспечения безопасности, которая основываются на предположении, что с ростом затрат на противодействие ЭМА ущерб от атак должен уменьшаться и, следовательно, должна быть такая точка, где сумма затрат и потерь от электромагнитной атаки (ЭМА) будет минимальной [1]. Пусть реализуется ЭМ атака на объект, оснащенный средствами электромагнитный защиты, и «нападающий» субъект на реализацию атаки затрачивает средства в объеме *Х*. Владелец инфокоммуникаций на создание системы обеспечения безопасности затратил средства в объеме . Соответственно, должна быть такая точка, где сумма затрат и потерь от атаки будет минимальна. Обозначим через  − результат, полученный нарушителем в результате ЭМА, например, продолжительность отказа в доступе к информации, вследствие электромагнитной деструкции базы данных. Выигрыш от деструкции будем определять функцией, где переменная  имеет размерность в часах. Потери владельца инфокоммуникационного ресурса будут определяться функцией . Обозначим прибыль нарушителя через функцию

 (1)

потери защитника через функцию

 (2)

Приравнивания к нулю частные производные выражений (1) и (2) можно определить уравнения, задающие точку равновесия. Отметим, что данная модель будет справедливой для каждой зоны защиты системы обеспечения ЭМБ. Вместе с тем для использования такой модели необходимо построить зависимости *l,* *f*, что представляет практические трудности. В связи с этим рассмотрим вероятностную модель распространения ЭМВ в зонной структуре системы обеспечения ЭМБ с полным перекрытием каналов распространения ЭМА.

Полагаем, что под *i*-й зоной безопасности понимается совокупность объектов защиты Oj, набора угроз  и набора средств противодействия .

Пусть угроза , реализуется с вероятностью  − условная вероятность того, что действие угрозы g¹i, распространяется через защитную зону и достигает объекта Oj*,* нанося ущерб . Кроме того действие угрозы может распространяться и далее, на связанные объекты, также нанося ущерб.

Вероятность успешной реализации атаки на каждый из объектов описывается следующими выражениями:

,

,

где: *P*1  − вероятность нарушения работы объекта O1, *P*2 − вероятность нарушения работы объекта O2.

Ожидаемый ущерб для каждого из объектов составит соответственно:

,

,

где  - ущерб от реализации угрозы в отношении объекта O*i*,.

Ожидаемый ущерб при отсутствии защитных барьеров может быть представлен равенствами:

,

,

Если затраты на создание зон защиты обозначить, как *С*1 и *С*2, то эффект от внедрения средств защиты описывается следующими соотношениями:

,

,

В результате, общий критерий эффективности системы обеспечения ЭМБ определяется как:

 .

Эту модель следует использовать для решения задачи выделения ресурсов (когда неизвестными параметрами являются ресурсы *Сi* обеспечивающие максимальную эффективность средств защиты) и задачи распределения ресурсов (когда требуется найти оптимальные значения *Сi* в пределах заданного суммарного ресурса *С0*). При этом предполагается, что появление каждой угрозы и ее последствия являются независимыми случайными событиями.

Обоснование применимости теоретико-игрового подхода в задаче   
реализации политики безопасности и задание игры.

В процессе реализации политики безопасности необходимо решить задачу выбора оптимального варианта зонной структуры системы обеспечения электромагнитной безопасности (ЭМБ). С одной стороны, увеличение уровня защищенности инфраструктуры инфокоммуникаций системы снижает риски ее эксплуатации, а с другой стороны требует вложения дополнительных средств.

Пусть определено разбиение всего множества угроз безопасности системы обеспечения ЭМБ на обобщенные угрозы, т.е. задано множество обобщенных угроз таких, что все угрозы безопасности, относимые к одной обобщенной угрозе, сходны по оказываемому на систему воздействию и объему ожидаемых потерь от реализации угрозы ЭМА.

Определены зоны защиты; для каждой пары «зона защиты − обобщенная угроза» могут быть получены численные оценки потерь в результате реализации данной угрозы.

В этом случае предлагается использовать теоретико-игровые модели в классе конечных игр двух игроков «защитника» и «нарушителя», для решения задачи анализа и выбора оптимального варианта структуры обеспечения ЭМБ [3]. Необходимо отметить, что в данной игре действиями «нарушителя» моделируются как преднамеренные воздействия на систему, так и случайные события, которые могут привести к нежелательным последствиям. Выбор конечных теоретико-игровых моделей определяется следующими характерными особенностями исследуемой задачи:

* наличие конфликта интересов «защитника» и «нарушителя»;
* присутствие фактора неопределенности;
* отсутствие достоверной статистической информации о действии нежелательных факторов;
* конечное множество вариантов зонных структур системы обеспечения ЭМБ;
* конечное множество обобщенных угроз;
* результаты действия нарушителя или случайных факторов можно оценить вещественным числом (например, оценка потерь от ЭМ атаки на систему), интерпретируемым как выигрыш одной из сторон.

Для построения игры необходимо определить стратегии игроков и функцию выигрыша. Пусть игрок I − «защитник», игрок II − «нарушитель» (источник угроз как случайных, так и ЭМА). Стратегии игрока I заключаются в выборе одного из вариантов системы обеспечения ЭМБ или отказе от каких-либо действий. Стратегии игрока II − реализация одной из множества обобщенных угроз или бездействие.

Допустим, что действия каждого из игроков являются однократными или могут быть сведены к некоторому суммарному однократному воздействию на систему. Это допущение позволяет использовать одношаговые игровые модели.

Рассмотрим антагонистические конечные одношаговые игры. В них значение выигрыша «защитника» равно по модулю и противоположно по знаку значению выигрыша «нарушителя».

Обозначим множество вариантов зонной структуры системы обеспечения ЭМБ через . Текущее или начальное состояние системы обеспечения можно описать в виде варианта , характеризуемого тем, что затраты на его осуществление равны 0. Тогда стратегия «защитника» (игрока I) будет заключаться в реализации одного из вариантов из множества .

Далее рассмотрим построение множества стратегий «нарушителя» (второго игрока). Оно формируется на базе множества  − множества обобщенных угроз, дополненного стратегией *,* обозначающей бездействие нарушителя. В итоге множество стратегий игрока II будет равно . Антагонистическая игра задается следующей тройкой

,

где:  − множество стратегий защитника:  множество стратегий нарушителя, − матрица выигрышей.

Пусть мощности множеств стратегий игроков равны: |Х| = *m*, |Y| = *n*.

Представим матрицу выигрышей в следующем виде:

 ,

где перед началом строк и столбцов указаны соответствующие элементы множеств X и У. В этой матрице использованы обозначения: − оценка потерь от реализации нарушителем *j*-й обобщенной угрозы, когда реализован *i*-й вариант системы обеспечения ЭМБ; − размер величины затрат на реализацию *i*-го варианта исследуемой системы.

Оценки потерь  могут быть получены по результатам анализа рисков (как правило, для их получения используется методы экспертных оценок). Если известен закон распределения вероятности появления случайных событий, создающих угрозу безопасности, то  математическое ожидание потерь.

В том случае, когда «нарушитель» ничего не предпринимает =0 (последний столбец матрицы Н).

Затраты на реализацию «защитником» последней стратегии (отказ от проведения дополнительных мероприятий по защите системы) также принимаются равными нулю.

Обе составляющие элемента матрицы **Н** взяты со знаком минус, т.к для игрока I («защитника») − это отрицательный выигрыш (потери).

Построенная антагонистическая игра отражает ситуацию наиболее пессимистичного прогноза, когда реальные возможности и цели нарушителя неизвестны, и считается, что он всемогущ и его цель − нанести максимальный вред. Если можно достоверно определить возможности «нарушителя» и ценность для него результатов ЭМА, то возможно использование биматричной игровой модели. Биматричная игра задается следующей «четверкой»:



,

где *X* и *У* − множества стратегий игроков I и II, *Н* − матрица выигрышей защитника; *Н*2 − матрица выигрышей нарушителя, которая формируется следующим образом:

,

где − оценка выигрыша «нарушителя» от реализации *j*-й обобщенной угрозы в отношении *i*-го варианта системы обеспечения ЭМБ; *-* оценка затрат «нарушителя» на реализацию этой угрозы.

Для обобщенных угроз, источниками которых являются случайные события (например, отказ оборудования), значение принимается равным нулю, а величину предлагаетсявзять равной по модулю и обратной по значению, соответствующему элементу матрицы выигрышей игрока I. Нули в последнем столбце матрицы Н2 соответствуют ситуации, когда «нарушитель» ничего не предпринимает.

По сравнению с антагонистической игровой моделью, биматричная модель отражает менее пессимистичный прогноз, основанный на наличии дополнительных знаний о «нарушителе». Соответственно, могут оказаться отличными от предыдущей модели и оптимальные стратегии.

Выбор оптимальной стратегии

Рассмотренные теоретики игровые модели реализации политики безопасности относятся к классу «игр против природы». Играми против природы называют модели принятия решения индивидом, когда функция выигрыша ему неизвестна, а точнее, известно лишь, что функция выигрыша «выбирается природой» из некоторого фиксированного множества. При этом неизвестны вероятности, с которыми выбирается та или иная функция. Задачей игрока I («защитника») является расстановка по приоритетам доступных ему стратегий и выбор из них наилучшей.

Пусть задача принятия решения задана в виде матрицы причем игрок выбирает строку в матрице, из которой и определяется его выигрыш. Тогда критерий оптимальности можно понимать как упорядочение "≥" на множестве альтернатив, считая, что наилучшей является максимальная по этому упорядочению альтернатива.

В теории принятия решений разработан ряд критериев оптимальности, в том числе критерий Вальда, в приложении к играм против природы. [3]. Рассмотрим антагонистическую игру Г=<Х, У, Н>, где X, У − множества стратегий игроков I и II соответственно, а *Н* − матрица выигрыша игрока I (проигрыша игрока II). В соответствии с принципом максимина игрок I стремится выбрать такую стратегию х°, чтобы при самом неблагоприятном для него выборе игрока II получить наибольший выигрыш, который определяется равенством:

,

где *Н(х,у)* − элемент матрицы выигрышей *Н*, соответствующий выбору игроком I стратегии «*х*», а игроком II − стратегии «у».

Для игрока II, выигрыш равен элементу матрицы Н со знаком минус. При использовании критерия Вальда, он предпочтет стратегию *у*, которая обеспечит для него наибольший выигрыш при наименее благоприятном выборе игрока I:

.

Ситуация (х, у) называется ситуацией равновесия в чистых стратегиях если для любых и выполнено неравенство седловой точки.

Рассмотренный теоретико-игровой подход к решению задачи построения формальных моделей политики безопасности системы обеспечения ЭМБ при практической реализации может использовать принципы кластеризации систем технической защиты телекоммуникаций от электромагнитных воздействий [2].

### Список литературы

1. Нестеров С.А. Проектирование инфраструктуры обеспечения информационной безопасности автоматизированных систем., С-П.,2002 г. − 134 с.
2. Акбашев Б.Б., Балюк Н.В., Кечиев Л.Н.Защита объектов телекоммуникаций от электромагнитных воздействий. − М.: Грифон, 2013 г. − 490 с.
3. Давыдов Э.Г. Исследование операций. − М.: Высшая школа, 1990 г. − 382 с.

*ОАО «Инженерно-маркетинговый центр «Концерн « Вега»*

*Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ)*

*Статья поступила 25.09.2014.*

*Mikheev V.A., Semin V.G.*

**Principles and methods of implementing the security policy of the system of electromagnetic security multifunctional information systems integrated structures of the military-industrial complex**

In the article the results of development of the methods of implementing policy-based security model of the system with the zonal structure of the organization system of electromagnetic security systems integrated structures of the military-industrial complex given. the existing concept of clustering systems of technical protection of telecommunications from electromagnetic influences.

**Key words: software; model; security policy; conflict; optimality; the choice**

*JSC «Engineering-marketing center of the Concern « VEGA».*

*National Research University «Higher school of Economics (NRU HSE)*