ОДИН ИЗ ПОДХОДОВ К ОПТИМИЗАЦИИ СОСТАВА КОМПЛЕКСА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Яхонтов Иван Владимирович,
Аспирант, Всероссийская государственная налоговая академия Минфина РФ
ivan.yakhontov@gmail.com

Аннотация. *В статье рассмотрены подходы к определению уровня совместимости средств защиты информации и выбору метода оптимизации комплекса технических средств защиты информации.*

Ключевые слова: *Информационная безопасность, технические средства защиты информации, электромагнитная совместимость, эффективность работы.*

ONE OF APPROACHES TO OPTIMIZATION OF STRUCTURE OF A COMPLEX OF MEANS OF PROTECTION OF INFORMATION

Yakhontov Ivan Vladimirovich,
Postgraduate student, Russian State Tax Academy Ministry of Finance RF

Abstract. *In article approaches to definition of level of compatibility of means of protection of information and a choice of a method of optimization of a complex of means of protection of information are considered.*

Keywords: *Information security, means of protection of information, electromagnetic compatibility, overall performance.*

Введение

В век информации особо актуальным кажется выражение, которое в свое время употребил Уинстон Черчилль, – «Кто владеет информацией, тот владеет миром». Желающих таким образом овладеть миром более чем достаточно, а значит и существует устойчивый спрос на информацию, полученную незаконным путем. В такой ситуации головная боль владельца информации – это ее надежная защита. Иными словами, и в информационной области идет извечная борьба снаряда и брони, нападающей стороны и защищающейся. Поэтому для каждого из нас так важна информационная безопасность.

В основном формирование «брони» информации идет за счет организационных, технических и программных средств защиты информации. Но далеко не всегда есть возможность использовать весь спектр технических средств защиты информации, как по причине ее себестоимости, так и по причине совместимости оборудования. В связи с этим встает вопрос об оптимизации комплекса средств защиты информации с целью сведения к минимуму их взаимного негативного влияния друг на друга и достижения максимально возможного уровня защиты информации.

1. Проблемы совместимости технических средств защиты информации

В средствах массовой информации и издаваемой литературе уделяется основное внимание освещению вопросов защиты информации, главным образом, от утечки и несанкционированного воздействия. При этом незаслуженно в стороне остается комплекс задач защиты информации от непреднамеренного воздействия. Действительно, если первые два направления отражают, в основном, задачи прямой защиты информации от умышленных действий заинтересованных или просто любопытных лиц, то последнее направление предполагает такую организацию пользования информацией и

техническими средствами ее обрабатывающими, чтобы ее не исказить и тем более не потерять. Иными словами комплекс мероприятий защиты информации от непреднамеренного воздействия предполагает внутреннюю организацию процесса обработки защищаемой информации собственником (или с его разрешения пользователем) с тем, чтобы по незнанию или другим причинам своими действиями не способствовать ее искажению или утрате. В перечне задач, решаемых в рамках этого направления защиты информации, доминирующее положение занимает проблема обеспечения электромагнитной совместимости технических средств (ЭМС ТС).

В современном мире наблюдается бурное развитие микроэлектроники и широкое внедрение ее изделий в состав практически всех технических средств (ТС), в том числе и обрабатывающих защищаемую информацию (в дальнейшем под техническим средством понимается, средство привлекаемое (либо совместно функционирующее) для обработки защищаемой информации). Наличие в составе таких средств элементов микроэлектроники, как правило, выполняющих управляющие функции, либо хранящие информацию непосредственно, существенно повышает их восприимчивость к воздействию электромагнитных полей или электромагнитных помех (ЭМП). Понятие "восприимчивость к помехам" определяет способность ТС, обрабатывающего информацию, при воздействии электромагнитных помех искажать содержание или безвозвратно утрачивать информацию, останавливать или нарушать процесс управления ее обработкой, изменять состав и последовательность функций средства и т.п., а также физического разрушения микроэлементов. Это обязывает при организации защиты информации решать задачи обеспечения ЭМС технических средств ее обрабатывающих.

В широком смысле решение проблемы ЭМС отдельного технического средства заключается в создании условий, при которых оно идеально совместимо с окружающей его средой или, другими словами, невосприимчиво к внешним помехам и не создает помехи для других средств. Во всех случаях электромагнитная помеха возникает при наличии трех факторов: ТС-источника помехи, среды ее распространения и технического средства, обладающего восприимчивостью к этой помехе (его часто называют рецептором).

В связи с этим при составлении перечня технических средств необходимо выполнить следующие условия:

- Использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
- Использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
- Использование сертифицированных средств защиты информации;
- Размещение объектов защиты на максимально возможном расстоянии от границ КЗ (контролируемой зоны);
- Размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах КЗ;
- Использование сертифицированных систем гарантированного электропитания (источников бесперебойного питания);
- Развязка цепей электропитания объектов защиты с помощью сетевых помехоподавляющих фильтров, блокирующих (подавляющих) информативный сигнал;
- Электромагнитная развязка между информационными цепями, по которым циркулирует защищаемая информация и линиями связи, другими цепями ВТСС, выходящими за пределы КЗ;
- Использование защищенных каналов связи.

2. Анализ функциональности комплекса средств защиты информации

Следующим шагом при построении комплекса защиты информации становится анализ возможностей как отдельных элементов комплекса, так и совместной работы элементов. Одним из наиболее качественных методов оценки эффективности является анализ структуры комплекса путем моделирования с использованием модифицированных сетей Петри.

Анализ моделей СЗИ проводился по следующим показателям:

- возможность определить вероятность реализации угрозы в зависимости от используемых средств защиты, и уязвимостей в них;

- возможность определить время реализации угрозы в зависимости от используемых средств защиты, уязвимостей в них;
- возможность моделирования параллельных процессов преодоления СЗИ;
- возможность моделирования скоординированных действий группы злоумышленников;

В работе [8] рассматриваются основные элементы защиты корпоративных систем (КС) от внешних и внутренних угроз. Отмечается, чтобы получить количественную оценку защищенности и определить уровень доверия можно использовать моделирования критических событий, используя вероятностные сети Петри.

Предлагаемый подход предполагает выполнение следующих процедур:

1) выделение и моделирование отдельных механизмов защиты от конкретных типов угроз;

2) вычисление вероятности реализации выбранных типов угроз;

3) определение общей вероятности нарушения безопасности объектов КС;

4) вывод уровня доверия к защищенной КС, исходя из рангов защищаемых объектов и вероятностей проявления угроз.

Полученные результаты можно использовать, как при оценке проектов, так и для контроля существующих КС. Анализ промежуточных значений поможет выявить слабые места и уязвимости в рассматриваемых корпоративных системах.

Реализация угрозы в корпоративной информационной системе предполагает поэтапное использование уязвимостей системы защиты информации в данной корпоративной информационной системе. Причинами возникновения уязвимостей СЗИ могут быть различные факторы — это могут быть уязвимости аппаратного и программного обеспечения, некорректно настроенная политика безопасности, уязвимости физической или технической подсистем защиты информации и т.д. Использование какой-либо уязвимости СЗИ дает злоумышленнику новые возможности в корпоративной информационной системе, однако уровень этих возможностей различается в зависимости от использованных уязвимостей. При этом не все уязвимости доступны злоумышленнику изначально. Часть из них может стать доступной для злоумышленника в процессе преодоления СЗИ как результат использования изначально доступных уязвимостей СЗИ.

Модель реализации угрозы, основывается на результатах работы [7] и описывает последовательное использование уязвимостей системы защиты информации, корпоративной системы и отображается в виде сети Петри, описанной кортежем представленным ниже:

$$N= (P1, T, I,W, M0)$$

где P1 – множество мест сети, T – множество переходов представляет собой фактически множество способов эксплуатации той или иной уязвимости, I – отношение между вершинами соответствующее дугам сети, W – функция задающая кратность дуги, W=1.

Для разрешения конфликтов используется предварительный выбор по вероятности срабатывания перехода, которая интерпретируется как вероятность выбора злоумышленником данного способа эксплуатации уязвимости. В модели время пребывания в состоянии интерпретируется как время необходимое злоумышленнику на эксплуатацию i-й уязвимости, при условии, что в дальнейшем он перейдет в j-ое состояние.

Анализ сети осуществляется по результатам моделирования. При моделировании до достижения одного из поглощающих состояний определяется среднее время, затрачиваемое на осуществление угрозы tугр, и вероятность P осуществления злоумышленником угрозы при отсутствии ограничений времени.

Архитектура программного комплекса реализующего модель оценки защищенности КИС на основе вероятностных сетей Петри, состоит из четырех блоков (рисунок 1).

Первый блок. Пользовательский интерфейс приложения. Пользователь формирует сеть Петри и вводит входные данные: наименование уязвимости, вероятность выбора данной уязвимости, вероятность успешной эксплуатации данной уязвимости, а также пользователь вводит параметры логнормального распределения для данной уязвимости и время моделирования.

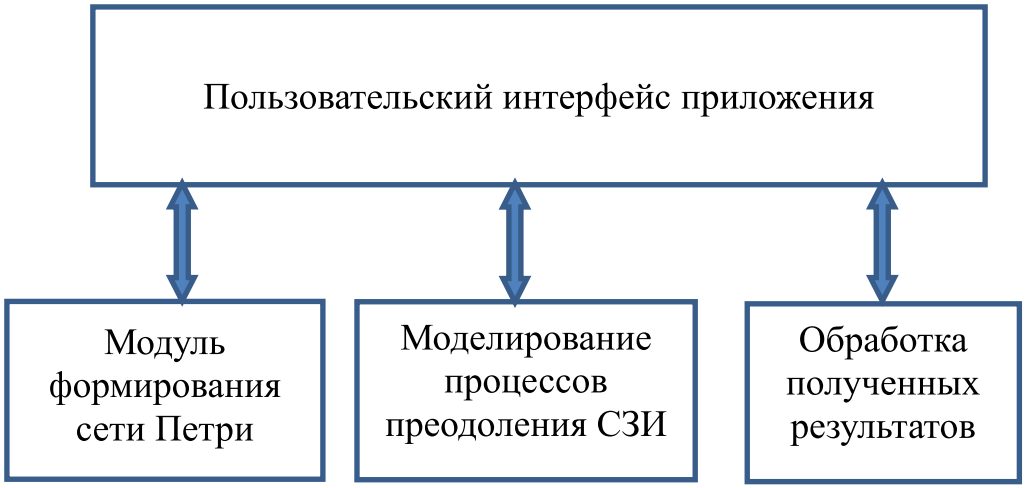

Рис. 1. Архитектура программного комплекса

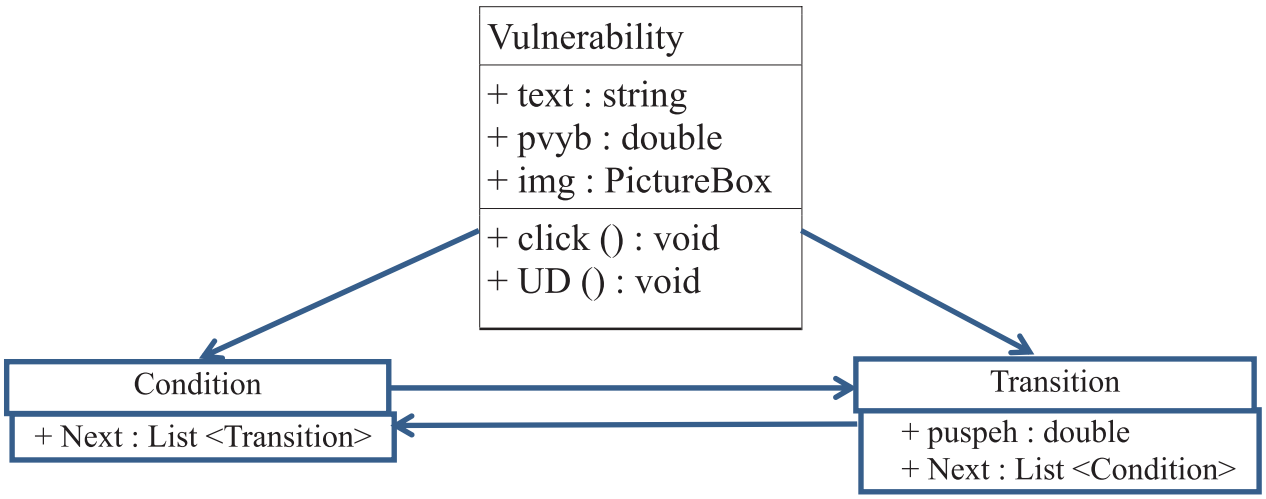

Рис. 2.

Второй блок. Моделирование процессов преодоления СЗИ. Осуществляется заданное число экспериментов по преодолению СЗИ, в результате чего накапливается статистика успешных и безуспешных атак, а также времени преодоления СЗИ.

Третий блок. Обработка полученных результатов. Осуществляется обработка полученной статистики экспериментов, на основании которой вычисляется вероятность и среднее время преодоления СЗИ.

В программном комплексе реализованы три класса (рисунок 2): родительский класс «Vulnerability» (уязвимость), класс «Condition» (состояние), класс Transition (переход).

Класс «Vulnerability» содержит поля:

- text: string содержит текстовое описание узла сети;
- параметр pvyb: double вероятность выбор этого узла;
- img: PictureBox параметр для графического представления узла;

В классе присутствуют два основных метода click():void вызывается при нажатии на графическое

представление узла, для выбора узла сети и второй метод UD():void вызывается при передвижении узла. В нем происходит пересчет координат центра верхней и нижней грани для отображения связей между узлами.

От класса «Vulnerability» (уязвимость) наследуются еще два класса «Condition» (состояние) и «Transition» (переход).

Класс «Condition» наследует все свойства и методы родительского класса «Vulnerability» и описывает дополнительные свойства характерные для состояния, это: Next: List<Transition> – список объектов класса «Transition» следующих за этим узлом.

Класс «Transition» так же наследует свойства и методы класса «Vulnerability» и имеет свои уникальные свойства, это puspeh: double – вероятность преодоления перехода и Next: List <Condition> – объекты класса «Condition» следующий за данным узлом сети.

На диаграмме показана связь между классами «Transition» и «Condition», от класса «Condition» к классу «Transition» идет ассоциация агрегация, так как к одному объекту класса «Condition» может идти несколько объектов класса Transition.

3. Оптимизация комплекса технических средств защиты информации

Теоретические основы выбора оптимального состава технических средств защиты информации (ТСЗИ) исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства.

Оптимальным будет считаться решение, которое в предполагаемых условиях наилучшим образом удовлетворит условиям рассматриваемой задачи. Оптимальность решения достигается за счет наиболее рационального распределения ресурсов, затрачиваемых на построение системы защиты информации.

При решении конкретной задачи оптимизации необходимо прежде всего выбрать математический метод, который приводил бы к конечным результатам с наименьшими затратами на вычисления или же давал возможность получить наибольший объем информации об иско мом решении. Выбор того или иного метода в значительной степени определяется постановкой задачи оптимизации, а также используемой математической моделью объекта оптимизации.

Выбор оптимального состава ТСЗИ усложняется рядом их особенностей, основными из которых являются:

- необходимость учета большого числа показателей ТСЗИ при оценке и выборе их оптимального варианта;
- преимущественно качественный характер показателей, учитываемых при анализе и синтезе ТСЗИ;
- существенная взаимосвязь и взаимозависимость этих показателей, имеющих противоречивый характер;
- необходимость использования информации, полученной экспертным путем;
- трудность получения исходных данных об ТСЗИ.

Указанные особенности делают практически невозможным применение традиционных методов оптимизации для решения задачи выбора оптимальных ТСЗИ.

Сложность процесса принятия решений, отсутствие математического аппарата приводят к тому, что при оценке и выборе альтернатив возможно (а зачастую просто необходимо) использовать и обрабатывать качественную экспертную информацию. Перспективным направлением разработки методов принятия решений при экспертной исходной информации является лингвистический подход на базе теории нечетких множеств и лингвистической переменной.

Теория нечетких множеств в очередной раз подтвердила одну известную всем исследователям истину: применяемый формальный аппарат по своим потенциальным возможностям и точности должен быть адекватен смысловому содержанию и точности исходных данных. Математическая статистика и теория вероятностей используют экспериментальные данные, обладающие строго определенной точностью и достоверностью. Теория нечетких множеств имеет дело с «человеческими знаниями», которые принято называть экспертной информацией.

При принятии решения о выборе оптимального варианта ТСЗИ возникает задача определения важности (веса) требований, предъявляемых к параметрам ТСЗИ. При решении практических задач обоснования требований и выбора оптимальных ТСЗИ возникает естественный вопрос рационального выбора метода определения весовых коэффициентов. Неправильный выбор метода приводит, как правило, к недостаточной обоснованности

производимых операций над малодостоверными исходными экспертными данными.

Факторы, влияющие на выбор метода оценки весовых коэффициентов.

1. Физическая сущность параметров и отношение между ними. Параметры определяются исходя из смысла провозглашенной цели. Далее необходимо определить степень взаимосвязей и взаимоотношений между ними, т.е. зависимости или независимости. Характер зависимости или независимости (независимость по полезности, по предпочтению, по безразличию и т.д.) влияет на выбор метода оценки.
2. Сложность проведения экспертизы и трудоемкость получения экспертной информации. Сложность и трудоемкость экспертизы определяется реальными условиями и возможностями ее проведения.
3. Степень согласованности мнений экспертов. Степень согласованности в первую очередь зависит от количества привлекаемых экспертов и уровня их квалификации. В то же время на нее влияет выбранный метод оценки весов. Так, наибольшую согласованность экспертов обеспечивает линейная свертка, наименьшую–непосредственная численная оценка весов, при этом ранжирование при всей его простоте позволяет получить весовые коэффициенты, достаточно точные и близкие к их значению, полученному методом линейной свертки.
4. Трудоемкость обработки экспертных данных. Этот фактор не является главным при современном уровне развития вычислительной техники. Однако применение сложных методов обработки экспертной информации может потребовать разработки специальной программы обработки, что повлияет на сроки проведения экспертизы.

Очевидно, что наиболее простыми методами с этой точки зрения являются ранговые и балльные методы. Учет вышеприведенных факторов позволяет выбрать рациональный вариант оценки весовых коэффициентов.

Сложность процесса принятия решений, отсутствие математического аппарата приводят к тому, что при оценке и выборе альтернатив возможно, (а зачастую просто необходимо) использовать и обрабатывать качественную экспертную информацию. Поэтому перспективным направлением разработки при выборе оптимальных ТСЗИ является лингвистический подход на базе теории нечетких множеств и лингвистических переменных.

Заключение

В статье освещены известные проблемы совместимости и методы анализа комплекса СЗИ. Освещена проблема выбора оптимального состава комплекса ТСЗИ и предложен наиболее перспективный подход разработки комплекса средств технической защиты информации.

Список литературы

1. “Математическое моделирование распределенных систем защиты информации”, Давыдова Е.Н. (Davidova_EN@mail.ru) http://swsys.ru/index.php?page=article&id=2764;
2. Сравнительный анализ моделей систем защиты информации. http://inf-bez.ru/?p=767;
3. Модель оценки защищенности корпоративной системы на основе вероятностных сетей Петри. http://inf-bez.ru/?p=769;
4. «Анализ защищенности корпоративных систем», А.А. Астаханов, открытые системы №07-08 2002.
5. «Технические средства и методы защиты информации» Под ред. А.П. Зайцева и А.А. Шелупанова, Москва, «Машиностроение» 2009г.
6. Мошников Е.А. Математические методы в поиске оптимальных технических средств защиты информации // Сборник докладов научной сессии ТУСУР 2011. - Томск: В-Спектр. - Ч.3. - с.222 — 224.
7. Арьков П.А. Построение модели процесса реализации угрозы в информационной системе на основе сетей Петри // Обозрение прикладной и промышленной математики. Том 15. М.: ООО «ОПиПМ», 2008. С.655.
8. Э.Р. Бейбутов Анализ защищенности корпоративных систем на основе вероятностных сетей Петри //Актуальные проблемы безопасности информационных технологий: Сборник материалов II Международной научно-практической конференции - 9-12 сентября 2008 - г. Красноярск – С. 53-56.