SENS'2006
Second Scientific Conference with International Participation
SPACE, ECOLOGY, NANOTECHNOLOGY, SAFETY
14 – 16 June 2006, Varna, Bulgaria

ЕДИН ПОДХОД ЗА ОЦЕНКА ЕФЕКТИВНОСТТА НА ИНФОРМАЦИОННА ЗАЩИТА

Бранимир Жеков

Институт за перспективни изследвания за отбраната –
Военна академия „Г. С. Раковски"
бул. Евлоги Георгиев № 82, 1504 София, България
E – mail: bzhekov@yahoo.com

Ключови думи: сигурност, информационна защита, системен подход, качество, ефективност.

Резюме: *В доклада е представен кратък анализ на възможността за прилагане на системния подход като методология за анализ и синтез на системи за информационна защита. Направена е оценка на приложимостта на съществуващата нормативна и методологическа база за оценка на ефективността на системи за информационна защита. Предложен е вероятностен подход за оценка на ефективността на системата за информационна защита, като са дефинирани съответни показатели на ефективността на системата и са дадени критерии за нейната оценка.*

Стремителното развитие и повсеместното внедряване на информационни и телекомуникационни технологии, през последното десетилетие, стана нов етап в икономическия и научно-техническия прогрес на човешката цивилизация, като при това все по-ясно се обозначава устойчивата тенденция към формиране на информационното общество.

Ръстът на информационния фактор в съвременния свят, масовото създаване, внедряване и експлоатация на информационни системи са предизвикали и продължават да предизвикват възникване на доста значително множество от проблеми в сферата на сигурността на личността, обществото и държавата.

Няма съмнение, че за защита на критически важните информационни системи се разработват и на практика са в наличност множество международни, национални, отраслови, фирмени и други стандартизационни, нормативно-технически и методически документи. Въпреки това обаче, няма еднозначен и категоричен отговор на най-важния въпрос – доколко предлаганото или реализираното решение е добро, каква е неговата планирана или реална ефективност. За съществуващото положение в областта на информационните системи, и по-конкретно в областта на информационната сигурност съществуват редица причини [6]:

- пренебрегване на системния подход като методология за анализ и синтез на системи за информационна защита;

- липсата на механизми за пълно и достоверно потвърждаване на качеството на системите за информационна защита;
- недостатъци на нормативната и методическата база по информационна сигурност, преди всичко в областта на показателите и критериите.

Системната парадигма

Реализацията на комплекса от мероприятия и мерки по осигуряване на информационна защита преди всичко е насочена към постигане на определена цел, т. е. тя има целево предназначение, което на формално ниво може да бъде представено посредством конкретна целева функция. При това може да се очаква, че желаемия резултат ще бъде постигнат в толкова по-голяма степен, колкото по-точно, по-еднозначно и по-конкретно е дефинирана самата функция, колкото по-задълбочено и по-прецизно са зададени и уточнени параметрите за нейното постигане, и колкото по-пълно са посочени съществуващите ресурсни, пространствено-времеви и други ограничения.

Ако целевата функция е с ниска степен на сложност и съществува сравнително висока вероятността за нейното постигане, т. е. тя може да бъде зададена чрез скаларен показател, то като правило нейната реализация се осъществява чрез използване на ограничен и сравнително несложен по състав и структура комплекс от мероприятия и мерки.

При разширяване на кръга от проблеми, които следва да бъдат решени за постигане на цялостна и комплексна информационна защита, целевата функция придобива многомерен, векторен характер. При това коефициентът на значимост на отделно взетите елементи се намалява, а се повишава ролята и значението на общосистемните задачи – определяне на оптималната структура и режимите на функциониране, организация на взаимодействието между отделните елементи и подсистеми, отчитане влиянието на външната среда и др.

Целенасоченото обединяване на крайното множество от взаимодействащи и взаимозаменяеми функционални елементи на информационната защита и отношенията между тях, формира тотално цяло с входни и изходни интерфейси, т.е. образува се системата на информационна защита. Отличително качествено свойство на агрегирането на отделните елементи на информационна защита в едно цяло (в система) е емергентността, което в случая изпълнява ролята на системообразуващ фактор, т. е. в новосъздаденото цяло се създават условия за възникване на т. нар. синергичен ефект. Същността на този ефект се свежда до появата на специфични, качествено нови свойства в цялото (системата), първоначално не присъщи за нито една от неговите (нейните) съставни елементи. Трябва да има предвид, че при агрегирането на елементите първостепенно значение имат само онези техни свойства, които определят взаимодействието помежду им и оказват влияние на системата като цяло, а също така и на изпълнението на дефинираната целева функция. При това посочените в [1] основни принципи за изграждане на съвременните сложни структурно-функционалните построения могат да бъдат приложени и към системата за информационна защита, съответно в морфологичен, функционален и информационен смисъл:

- *съгласуваност* – структурно-функционална стандартизация, унификация, причинно-следствена и пространствено-времева свързаност;
- *ортогоналност* – модулност, агрегативност и автономност;
- *съответствие* – максимизация на критериалната ефективност по пълнота, достоверност, точност, надеждност;
- *икономичност* – ефект, ефективност, целесъобразност и полезност;
- *прозрачност* – обща наблюдаемост и управляемост;

- *общност* – циклична завършеност, затвореност, устойчивост и сходимост;
- *откритост* – максимална потребителска и йерархично-управленска достъпност;
- *пълнота* – максимизация на функционалната ефективност при структурно-параметрична ограниченост;
- *реверсивна каузалност* – интелигентни положителни обратни връзки на управлението, надстроени над функционалната хомеостаза на системата.

От приведените по-горе принципи, принципът "икономичност" в смисъл ефект, ефективност, целесъобразност и полезност на системата за информационна защита представлява определен интерес от теоретична и практична гледна точка, поради което е обект на по-нататъшните съждения.

Като се има предвид, че в основата на реализацията на системния подход лежи циклично-реверсивното приложение на методите на анализа и синтеза [2], то резултативно решение при проектирането и изследването на системата за информационна защита не може да бъде получено само чрез логически съждения за нейното поведение при различни ситуации и условия. Преобладаваща част от проблемите, имащи конкретна практическа насоченост, изискват количествени, а не качествени оценки на съответните характеристиките. Необходими са конкретни данни, които да разкриват свойствата на системата. В този смисъл обикновено възниква остра необходимост от количествена мярка за качеството на съответствие.

За оценка на качеството на съответствие на системата за информационна защита в редица случаи е целесъобразно използването на едно от основните свойства на системата, а именно ефективността на нейното функциониране, под която съгласно [3], се разбира някаква количествена характеристика на качеството и обема на изпълняваната от системата работа по информационната защита, или с други думи степента на съответствие на резултатите от защитата на информацията на поставената цел. Като количествена характеристика на качеството на съответствие, ефективността е непосредствено свързана с други системни свойства, като качество, надеждност, устойчивост, управляемост, шумозащитеност. Поради това количествената оценка на ефективността позволява да се измерват и обективно да се анализират основните свойства на системата за информационна защита на всички етапи от нейния жизнен цикъл.

Акредитация, сертификация, качество

Информационните системи, в които се създава, обработва, съхранява и пренася класифицирана информация, подлежат на задължителна акредитация в съответствие с действащите законови и нормативни документи. При това обаче възниква въпроса доколко сертификацията на съответствие на изискванията е най-добрият инструмент, с каква степен на достоверност се потвърждава това съответствие и дава ли тя необходимите гаранции. И ако се допусне, че степента на достоверност все пак е известна, означава ли това, че този термин е еквивалентен на вероятностно-статистическото разбиране на това понятие. Нещо повече, контрола и отговорността за достоверността на резултатите е непосредствено възложена на съответните сертифициращи органи (лаборатории), т. е. те сами извършват измерванията и сами се контролират. При една такава ситуация, нормативното изискване за осигуряване на определена достоверност на резултатите от изпитванията на отделните средства, и още повече на цялата

система за информационна защита, може ми ще остане трудно осъществима декларация.

Неопределеността на постигнатия резултат се засилва и от факта, че много често заявителите на системи за информационна защита не са запознати в достатъчна степен с функционалните възможности на отделните средства и със степента на тяхното влияние върху общото ниво на информационна сигурност и извършват необосновани разходи. В резултат на това, заявителя не винаги получава това, от което реално има нужда и не е в състояние обективно да провери и оцени качеството и ефективността на предложеното решение.

Както беше посочено по-горе, затрудненията при обективното потвърждаване на ефективността на информационната защита произтичат както от съществуващата нормативна база, така и от недостатъчно разработената система от показатели за информационна сигурност [4]. Не удовлетворява напълно потребностите и съществуващата система от критерии за информационна сигурност, в това число и такива, като ефективност на системата за информационна защита. Към сериозните проблеми следва да бъде отнесено и честото пренебрегване на стохастичната природа на събитията и явленията, които възникват в процеса на защита на информацията, абстрахиране от тяхното икономическо съдържание в нормативен, методически и приложен аспект [5].

По този начин, съществуващите национални и международни стандарти и документи на тяхна основа не дават отговор на редица ключови въпроси [6]:

- Как да се създаде информационна система, която да притежава информационна защита със зададено, измеримо, обективно проверяемо ниво?
- Как на практика да се организира режимът на информационна защита и той да се поддържа в условията на постоянно изменящата се външна среда и структура на самата система?
- Какво е реалното ниво на сигурност и колко е ефективна системата за информационна защита?

Показатели и критерии

Тъй като качеството на който и да е обект, в това число и системата за информационна защита, съгласно [7], се проявява само в процеса на неговото използване по предназначение, т.е. при неговото целево функциониране, то най-обективната оценка на този обект е оценката по ефективността на неговото използването.

Проектирането, организацията и използването на системата за информационна защита фактически са свързани с неизвестни събития в бъдещето и поради това винаги съдържат елементи на неопределеност. С реализацията на проекта, нивото на тази неопределеност се намалява, но никога ефективността на системата за информационна защита не може да бъде адекватно изразена и описана чрез детерминирани показатели. Процедурите по изпитване, сертифициране или лицензиране не отстраняват напълно неопределеността на свойствата на системата за информационна защита или на отделните нейни елементи и не отчитат случайния характер на атаките. Ето защо обективна характеристика на качеството на системата за информационна защита – степента на нейната адаптируемост за достигане на зададеното ниво на информационна сигурност в условията на реално въздействие на случайни фактори, може да служи вероятността, характеризираща степента на възможностите конкретната система за информационна защита, при зададен комплекс от условия. Съгласно общата теория на системите такава вероятност се нарича вероятност за достигане на целта на

операцията или вероятността за изпълнение на поставените задачи пред системата. Дадената вероятност следва да бъде поставена в основата на комплекса от показатели и критерии за оценка на ефективността на системата за информационна защита. При това в качеството на критерии за оценка могат да се използват понятията годност и оптималност, като годност означава изпълнение на всички изисквания, поставени към системата за информационна защита, а оптималност – достигане на една от характеристиките на оптимално значение при спазване на ограниченията и условията на другите свойства на системата. При избора на конкретен критерий е необходимо той да бъде съгласуван с целта, поставена пред системата за информационна защита. В табл.1 са дадени са дадени възможни показатели за ефективност, а в табл.2 – възможни критерии за ефективност на система за информационна защита [6].

Таблица 1

№	Изисквания към системата	Показатели за ефективност
1.	Поява или отсъствие на събитие	Вероятност на събитието
2.	Достигане на зададени характеристики	Вероятност за достигане на резултат не по-нисък от зададено ниво
3.	Отклонение от зададени характеристики	Средно квадратично отклонение на резултата от зададена стойност
4.	Осигуряване на гарантирано ниво на характеристики	Квантил на зададено ниво на гаранция
5.	Не са предявени	• Математическо очакване на резултат • Дисперсия на резултат • Среден риск

Таблица 2

№	Концепция за ефективност на системата	Критерии за ефективност
1.	Годност	• Приемлив резултат • Допустима гаранция • Допустим гарантиран резултат
2.	Оптималност	• Най-добър резултат • Най-добър среден резултат • Най-голяма вероятност за гарантиране на резултат • Най-голям гарантиран резултат

В съвременните нормативни документи по информационна защита, както е известно, основно се използва квалификационният подход. Значително по-конструктивни на практика са вероятностните методи, намерили широко разпространение в други области на науката и практиката. Съгласно тези методи, нивата за гарантиране на сигурността на системата за информационна защита се трансформират в доверителни вероятности на съответните оценки на показателите. За решаването на тази задача може да се използва теорията на статистическите решения [7], позволяваща да се определят оптимални нива на гарантиране на сигурността.

Преди всичко, оценката на оптималното ниво на гарантиране на сигурността в определена степен зависи от щетата, свързана с грешката при избора на

конкретното значение на показателя на ефективността. Освен това, за получаване на числени оценки на риска е необходимо да бъде известно разпределението на множество случайни величини. В редица практически случаи такива оценки е възможно да бъдат получени по резултатите от активните одити на системите за информационна защита или с помощта на симулационно моделиране.

Симулационно моделиране

Както е известно, целта на програмната симулация е чрез проиграване на създадените за целта симулационни модели да се изследва поведението на обекти при различни параметри на въздействуващите фактори и анализиране ефекта, който тази промяна оказва върху крайния резултат, при характерните за това предимства – изследването се извършва в лабораторни условия, лисват проблеми, свързани с предизвикване на възможни реални повреди, наличие на определена икономическа ефективност.

Симулационото моделиране освен за оценка на разпределението на случайни величини, необходими за прилагане на теорията на статистическите решения, може да намери полезно практическо приложение, съгласно [8], за изследване на ефективността на информационната защита и по конкретно при анализ на риска от потенциални атаки, оценка на вероятните щети, оценка на надеждността на топологията, симулиране на атаки и др.

Съществена роля при използване на симулациите в областта на информационната защита имат инструментите за моделиране на мрежи. Техен основен представител е продукта Opnet (Optimized Network Engineering Tool) на фирма OPNET Technologies Inc. и по-конкретно неговия модул, предназначен за анализ на мрежовата сигурност, NetDoctor.

Независимо от сложността на мрежовите симулатори, симулацията остава един добър подход за анализ на процесите в реалните мрежови конфигурации и за оценка на ефективността на тяхната защита.

Заключение

Прилагането на системния подход при получаване на количествени оценки на ефективността на информационната защита създава условия за конкретна обективност и значимост на резултатите. Вероятностният характер на процесите, голямата динамика на технологичните иновации и разнородните заплахи предопределят симулационното моделиране в областта на информационната защита като един перспективен и ценен подход.

Литература

1. Blaauw, G. Coputer architecture. Electronische Rechenanlagen. 14, №4, 1972.
2. Семерджиев Ц. Инструменти за стратегическо ръководство “C^4I”. С., Софттрейд София, 2001.
3. Ушаков И. А. Надежднсть технических систем. М., Радио и связь, 1985.
4. ISO/MEC 15408-99 “ Criteria of an estimation of safety of information technologies.”
5. Баутов А. Стандарты и оценка эффективности защиты информации. Доклад на Третьей Всероссийской практической конференции “Стандарты в проектах современных информационных систем”, М., 2003.
6. Баутов А. Эффективность защиты информации. Открытые системы №7, 2003.
7. Петухов Г. Основы теории эффективности целенаправленных процесов. Част 1, Методология, методы, модели. М., МО, 1989.
8. Пугачев В. Теория вероятностей и математическая статистика. М., Наука, 1979.

9. Saunders, J. *Simulation Approaches in Information Security Education.* Presented at the National Colloquium on Information Systems Security Education, Seattle, WA, 2002.