УДК 004.056.5+621.3

к.т.н. Закутный А.С.,
Лопухов А.С.
(ДонГТУ, г. Алчевск, Украина)

ОЦЕНКА ЭФФЕКТИВНОСТИ И АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Наведено результати теоретичних досліджень аналізу захищеності систем захисту інформації. Сформульовано вимоги до показників і критеріїв ефективності систем захисту інформації.

Ключові слова: *система захисту інформації, інформаційна система.*

Приведены результаты теоретических исследований анализа защищенности систем защиты информации. Сформулированы требования к показателям и критериям эффективности систем защиты информации.

Ключевые слова: *система защиты информации, информационная система.*

К уровню информационной безопасности различных компаний, предприятий и организаций предъявляются высокие требования. При этом требования и задачи защиты информации могут значительно отличаться. Их формулировка и решение является сложной организационно-технической задачей, требующей комплексного подхода. Решение каждой подзадачи может иметь несколько решений, имеющих различную эффективность, сложность и стоимость реализации и поддержки. В связи с этим актуальной является проблема оценки эффективности выбранных и принятых решений защиты информации.

В настоящее время существует много работ, посвященных проблемам защиты компьютерной безопасности в информационных системах обработки информации и сетях передачи данных [1-8]. Результаты, которых изложены в работах многих отечественных и зарубежных ученых. Среди них можно отметить таких авторов, как Е.С. Вентцель, В.Ю. Гайкович, В.А. Галатенко, В.А. Герасименко, В.И. Гарбарчук, Ю.В. Демченко,В.И. Завгородний, В.К. Задирака, А.Г. Карпов, В.В. Лебедев, В.В. Мельников, В.С. Михалевич, А.Н. Назаров, А.С. Олексюк, А.Ю. Першин, А.З. Пескозуб, А.П. Пятибратов, В.К. Размахнин, С.П. Расторгуев, Ю. Самохин, И.В. Сергиенко, А.В. Соколов, С.Е. Ста-

ленков, Г.В. Фоменков, Ю.В. Щеглов, С. Шатт, Д. Шепелявый, Г.Е. Шепитько, В.В. Шураков, В.Ф. Шаньгин, Н.А. Маслова, В.В. Домарев и многих других.

Однако многие методологические, методические и практические аспекты защиты информации носят дискуссионный характер. Это связано с малоизученностью некоторых аспектов защиты, вызванных сложностью рассматриваемых систем, постоянно изменяющимся перечнем угроз и отсутствием единого подхода к построению и анализу систем защиты. Например, в компьютерной вирусологии, несмотря на многочисленные специализированные конференции и регулярные семинары, работы множества фирм, занимающихся разработкой антивирусного программного обеспечения, до сих пор нет общеутвержденной и стандартизованной классификационной таблицы вирусов. Также недостаточно хорошо проработаны система оценки информационной безопасности и критерии защищенности, что делает поставленную задачу необходимой и актуальной.

Большинство моделей, оценивающих эффективность систем защиты информации (СЗИ) не дают численных методов определения величины защищенности и вероятности несанкционированного проникновения в информационную систему (ИС). Оценка таких показателей обычно дается экспертами-специалистами в области информационных технологий.

Управление рисками в основном учитывает риски с высокой вероятностью появления в период эксплуатации ИС. Такие риски обычно приносят незначительный или легко устранимый ущерб (вирусные атаки), но на практике основное внимание уделяется рискам с большим ущербам и с малой вероятностью. Это зачастую ведет к неоправданно большим затратам при построении СЗИ. Выбор оптимальной модели с точки зрения «цена-качество» представляет очень сложную задачу.

На основании модели угроз разрабатывается наиболее выгодный (оптимальный) вариант построения СЗИ, который представляется в виде набора угроз и мероприятий по защите информации. В общем такую модель можно изобразить в виде следующей схемы, приведенной на рисунке 1.

В моделях защиты информации выделяют коэффициент опасности события ($К_{ос\,i}$) от ущерба ($У_i$), вызванного несанкционированными действиями ($Н_i$). При несанкционированных действиях ущерб наступает независимо от издержек, вложенных в создание автоматизированной системы. Таким образом, задачей создания СЗИ является нейтрализация или минимизация ущерба от несанкционированных действий.

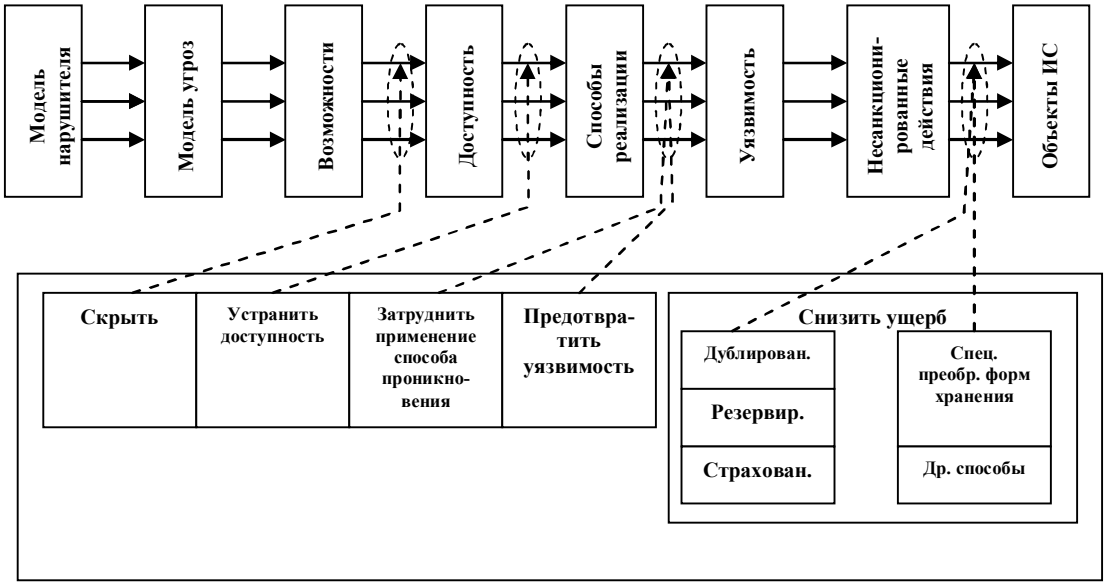

Рисунок 1 - Схема защиты информации
в автоматизированной системе обработки информации

Задача обеспечения информационной безопасности состоит в разработке модели представления системы мер, которые позволили бы решать задачи создания, использования и оценки эффективности СЗИ. В упрощенном виде модель СЗИ представлена на рисунке 2.

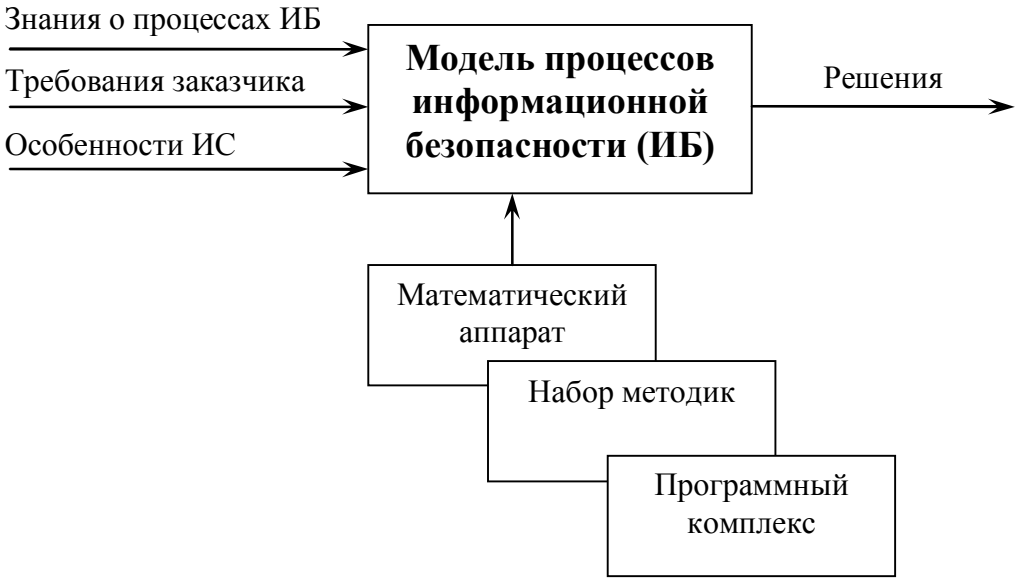

Рисунок 2 – Модель СЗИ

Основной задачей модели является обеспечение процесса создания системы информационной безопасности за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

Специфическими особенностями решения задачи создания систем защиты являются:

- неполнота и неопределенность исходной информации о составе ИС и характерных угрозах;

- многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей (требований) СЗИ;

- наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СЗИ.

Такая модель должна удовлетворять целый ряд требований.

1. Использоваться в качестве:
   - руководства по созданию СЗИ;
   - методики формирования показателей и требований к СЗИ;
   - инструмента для оценки СЗИ.
2. Обладать свойствами:
   - универсальность;
   - комплексность;
   - простота использования;
   - наглядность.
3. Позволять:
   - задавать различные уровни защиты;
   - получать количественные оценки;
   - контролировать состояние СЗИ.

Эффективность СЗИ выражается в отношении полезных результатов ее функционирования к затраченным ресурсам на ее создание. Основным показателем эффективности СЗИ является коэффициент эффективности $К_{эф}$, как показатель её приближения к предельным издержкам на СЗИ:

$$K_{эф} = \frac{C_{СЗИ}}{M_{СЗИ}}, \qquad (1)$$

где $С_{СЗИ}$ – затраты на создание СЗИ;

$М_{СЗИ}$ – предельные издержки на СЗИ.

Коэффициент $К_{эф}$ применяется для расчетов «эффективность-стоимость». Для систем защиты информации не имеющих коммерческий характер, эффективность зависит от показателя «ущерб-стоимость», т.е. с помощью СЗИ увеличиваются затраты злоумышленника и его риски на взлом информации. Таким образом, эффективней будет та система защиты, в которой при наименьших затратах на ее создание требуются наибольшие затраты на ее взлом.

Сформулируем общие подходы к количественной оценке эффективности СЗИ.

В соответствии с современной теорией оценки эффективности систем, качество любого объекта, в том числе и СЗИ, проявляется лишь в процессе его использования по назначению (целевое функционирование), поэтому наиболее объективным является оценивание по эффективности применения.

Проектирование, организация и применение СЗИ фактически связаны с неизвестными событиями в будущем и поэтому всегда содержат элементы неопределенности. Кроме того, присутствуют и другие причины неоднозначности, такие как недостаточно полная информация для принятия управленческих решений или социально-психологические факторы. Поэтому, например, этапу проектирования СЗИ естественным образом сопутствует значительная неопределенность. По мере реализации проекта ее уровень снижается, но никогда эффективность СЗИ не может быть адекватно выражена и описана детерминированными показателями.

Процедуры испытаний, сертификации или лицензирования не устраняют полностью неопределенность свойств СЗИ или ее отдельных элементов и не учитывают случайный характер атак. Поэтому объективной характеристикой качества СЗИ — степенью ее приспособленности к достижению требуемого уровня безопасности в условиях реального воздействия случайных факторов, может служить только вероятность, характеризующая степень возможностей конкретной СЗИ при заданном комплексе условий. В общей теории систем такая характеристика называется вероятностью достижения цели операции или вероятностью выполнения задачи системой. Данная вероятность должна быть положена в основу комплекса показателей и критериев оценки эффективности СЗИ. При этом критериями оценки служат понятия пригодности и оптимальности. Пригодность означает выполнение всех установленных к СЗИ требований, а оптимальность — достижение одной из характеристик экстремального значения при соблюдении ограничений и условий на другие свойства системы. При выборе конкретного критерия необходимо его согласование с целью, возлагаемой на СЗИ.

Обычно при синтезе системы возникает проблема решения задачи с многокритериальным показателем. Некоторые авторы рассматривают показатели эффективности, которые предназначены при решении задачи сравнения различных структур СЗИ. Предлагается также использовать показатели эффективности вероятностно-временного характера, имеющие смысл функций распределения. В частности, к ним относятся вероятность преодоления системы защиты информации за некоторое время.

Оценку гарантий защиты также необходимо сформулировать в количественной форме.

В современных нормативных документах по информационной безопасности, используется, как известно, классификационный подход. Гораздо более конструктивными являются вероятностные методы, нашедшие широкое распространение в практике обеспечения безопасности в других прикладных областях. В соответствии с этими методами уровни гарантий безопасности СЗИ трансформируются в доверительные вероятности соответствующих оценок показателей. Для решения данной задачи можно рекомендовать теорию статистических решений, позволяющую находить оптимальные уровни гарантий безопасности.

Во-первых, оценка оптимального уровня гарантий безопасности в определяющей степени зависит от ущерба, связанного с ошибкой в выборе конкретного значения показателя эффективности. Во-вторых, для получения численных оценок риска необходимо знать распределения ряда случайных величин. Это, конечно, в определенной степени ограничивает количественное исследование уровней гарантий безопасности, предоставляемых СЗИ, но, тем не менее, во многих практических случаях такие оценки можно получить, например, с помощью имитационного моделирования или по результатам активного аудита СЗИ.

Обобщенные данные о возможных показателях эффективности приведены в таблице 1, а критериев — в таблице 2.

Таблица 1 - Возможные показатели эффективности СЗИ

Требования к СЗИ	*Вид показателя эффективности СЗИ*
Наступление или отсутствие события	Вероятность события
Достижение требуемых характеристик	Вероятность достижения события не ниже требуемого уровня
Отклонение от заданных характеристик	Средне квадратичное отклонение от требуемого результата

Таблица 2 - Возможные критерии эффективности СЗИ

Концепция эффективности СЗИ	*Критерии эффективности*
Пригодность	1. Приемлемый результат
	2. Допустимая гарантия
Оптимальность	1. Наилучший результат
	2. Наилучший средний результат
	3. Наибольший гарантированный результат

Для наглядного представления текущего состояния эффективности СЗИ целесообразно использовать лепестковую диаграмму, изображенную на рисунке 3. Маркеры отображающие значение защищенных параметров в процентах.

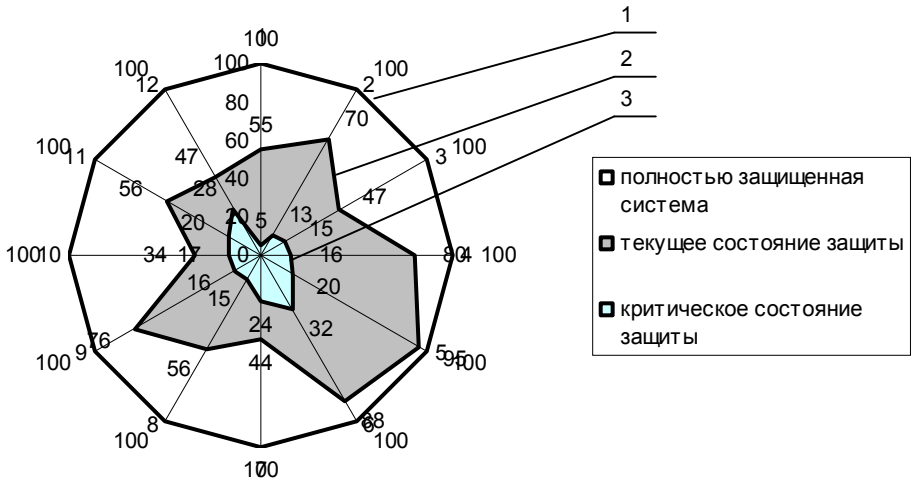

Рисунок 3 – Лепестковая диаграмма оценки защищенности СЗИ:
1 – полностью защищенный параметр системы;
2 – текущее состояние защищенности параметра системы;
3 – критическое состояние защищенности параметра системы

Из приведенной диаграммы видно, что СЗИ работает эффективно, так как текущее состояние всех параметров защищенности больше соответствующих критических. Средневзвешенный нормированный показатель степени защищенности ИС равен 62%, что больше на 44% соответствующего среднего критического параметра системы. Важно также отметить максимальную и минимальную разность между текущим и критическим параметром системы. Максимальная разность составляет 75% по 5 параметру, а минимальная 17% по 10 параметру. Таким образом можно оценить избыточные и недостаточные меры защиты. Такой анализ позволяет более оптимально использовать выделенные ресурсы, особенной при использовании критерия “эффективность – стоимость”.

Многочисленные методы оценки эффективности и защищенности СЗИ имеют некоторые недостатки. Для решения данной задачи можно воспользоваться несколькими критериями, а затем усреднить количественные показатели с различными коэффициентами доверия для разных методов. Еще одним вариантом решения может быть использование методов нечеткой логики, как для усреднения разных методов оценки, так и для перевода нечеткого лингвистического мнения эксперта в количественную величину.

Выводы:

1. Анализ работ СЗИ показывает, что в настоящее время не существует общепринятых оценок защищенности информационных систем.
2. В статье сформулированы основные требования к системам защиты информации.
3. Перспективным способом оценки состояния защищенности информационных систем являются методы нечеткой логики.
4. Для наглядного представления состояния СЗИ в режиме on-line контроля, осуществляемого системным администратором СЗИ, предлагается использовать лепестковую диаграмму.

Библиографический список

1. Баутов А. Экономический взгляд на проблемы информационной безопасности / А. Баутов // Открытые системы. - 2002. - № 2.

2. Горбунов А. Выбор рациональной структуры средств защиты информации в АСУ / А. Горбунов, В. Чуменко // - Режим доступа : http://kiev-security.org.ua/box/2/26.shtml.

3. Защита информации. Основные термины и определения : ГОСТ Р 50922-96.

4. Критерии оценки безопасности информационных технологий : ИСО/МЭК 15408-99.

5. Козлов В. Критерии информационной безопасности и поддерживающие их стандарты: состояние и тенденции / В. Козлов // Стандарты в проектах современных информационных систем : сборник трудов II-й Всероссийской практической конференции. Москва, 27-28 марта 2002 года. – 2002.

6. Липаев В. Формирование и применение профилей открытых информационных систем / В. Липаев, Е. Филинов // Открытые системы. - 1997. - № 5.

7. Хмелев Л. Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем / Л. Хмелев // «Безопасность информационных технологий» : Труды научно-технической конференции, Пенза, июнь 2001. - 2001

8. Маслова Н. А. Методы оценки эффективности систем защиты информационных систем / Н. А. Маслова // - Режим доступа : http://www.nbuv.gov.ua/portal/natural/II/2008_4/JournalAI_2008_4/Razdel3/07_Maslova.pdf.

Рекомендовано к печати к.т.н., проф. Паэрандом Ю.Э.