УДК 65.012

А.А.СЕРКОВ, докт.техн.наук, проф., ХНУВД, Харьков;
В.Я.ПЕВНЕВ, канд.техн.наук, зав. кафедрой, ХНУВД, Харьков;
Л.Ю.НЕСТЕРЕНКО, бакалавр, ХНУВД, Харьков

МЕТОДИКА ВЫБОРА ОПТИМАЛЬНОЙ КОНФИГУРАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Розглянуто критерії ефективності систем захисту інформації. Наведено етапи побудови систем технічного захисту інформації. Описано основні способи підвищення надійності технічних систем. Сформульована математична постановка задачі обрання конфігурації системи. Запропонована методика побудови системи захисту інформації, яка задовольняє завданим вимогам щодо надійності із урахуванням завданих обмежень.

The criteria of efficiency of the systems of protection to information are considered. The stages of the building of the systems of technical protection to information are presented. They ways of increasing to reliability of the technical systems are shown. Mathematical statement of the problem configuring systems is worded. The methods of the building of the system of protection to information, satisfying given requirements on reliability with provision for brought forth restrictions are offered.

Постановка проблемы. Одной из самих востребованных задач, с точки зрения пользователя, является задача обеспечения заданного уровня безопасности системы (ЗУБС) при минимальных затратах. ЗУБС следует обеспечивать набором приборов, которые перекрывают весь спектр возможных угроз, как по утечке информации, так и по ее искажению.

Анализ литературы. В современной литературе достаточно много внимания уделяется надежности защиты информации (ЗИ). Однако при этом отсутствует оценка надежности защиты с точки зрения надежности аппаратуры и программных средств. Этот аспект затрагивается в работах [1,2], однако он рассматривается с точки зрения средств нападения.

Цель статьи – разработка методики выбора оптимальной конфигурации систем.

Критерии эффективности. Информация с ограниченным доступом (ИСОД) в процессе информационной деятельности может подвергаться воздействию угроз ее безопасности. В связи с этим возможна утечка или нарушение целостности информации. Склонность ИСОД изменяться под действием угроз определяет ее уязвимость. Способность систем ЗИ (СЗИ) противостоять действию угроз определяет эффективность защиты ИСОД. При разработке и оценке качества СЗИ необходимо использовать критерии эффективности. Существует несколько вариантов этих критерий [3]:

– достижение необходимого уровня защиты ИСОД при минимальных затратах и допустимом уровне ограничений видов информационной деятельности (ИД);

– достижение необходимого уровня защиты ИСОД при допустимых затратах и заданном уровне ограничений видов ИД;
– достижение максимального уровня защиты ИСОД при необходимых затратах и минимальном уровне ограничений видов ИД;
– достижение минимального времени восстановления при сбоях и отказах, которые вызваны нарушением информационных ресурсов.

Защита информации, которая не является государственной тайной, обеспечивается, как правило, использованием первого или второго критерия. ЗИ, которая составляет государственную тайну, обеспечивается, как правило, использованием третьего варианта.

С целью противостояния утечки или нарушения целостности ИСОД используют техническую защиту информации (ТЗИ). Цель ТЗИ может достигаться построением системы ЗИ, которая является организованной совокупностью методов и способов обеспечения ТЗИ. При построении системы защиты информации (СЗИ) необходимо ТЗИ выполнять поэтапно:

– 1 этап – определение и анализ угроз;
– 2 этап – разработка СЗИ;
– 3 этап – реализация плана ЗИ;
– 4 этап – контроль функционирования и управления СЗИ.

Математическая постановка задачи. При построении любой технической системы следует учитывать возможность выхода из строя любого из компонентов системы. В таком случае используют понятие надежности системы. При этом под надежностью понимается возможность системы сохранять во времени в установленных границах значения всех параметров, которые характеризуют способность выполнять нужные функции в заданных режимах и условиях использования, технического обслуживания, ремонта и т.д. [3,4]. Надежность системы можно обеспечить двумя способами. Первый способ – создание надежных приборов, использованных для построения системы, второй – резервирование приборов с низкой надежностью. В первом случае выход из строя, хотя б одного прибора ведет к выходу из строя всей системы. Во втором случае выход из строя одного из дублированных приборов не воздействует на работоспособность всей системы.

Таким образом, критерием эффективности для разрабатываемой системы [5] будет минимизация выхода из строя системы защиты информации при заданной стоимости и обеспечении заданного уровня ЗИ. Математическая постановка задачи будет выглядеть таким образом:

$$\Xi = \min\left\{1 - \prod_{i=1}^{N}\left(1 - x_i^{x_j^i}\right)\right\}$$

при ограничениях

$$\sum_{i=1}^{N} d_i \, x_j^i \le D; \quad \{x_1,\ldots,x_N\} \ge X,$$

где: Ξ – вероятность отказа СЗИ; x_i – вероятность отказа i-го прибора; d_i – количество приборов i-го типа в системе; D – максимальное количество приборов в системе; X – минимальное количество типов приборов в системе, необходимое для решения поставленной задачи; x_i – типы приборов.

Методика выбора конфигурации системы.

Предлагаемая методика основывается на определении максимума надежности при ряде принятых ограничений.

Порядок действий выглядит следующим образом.

1. Обследовать объект, подлежащий защите, на предмет возможных каналов утечки информации и угроз.
2. Определить минимальный перечень оборудования, позволяющий решить поставленную задачу.
3. Определить надежность и стоимость выбранных приборов, обеспечивающих заданный уровень ЗИ.
4. Рассмотреть ограничения, выдвинутые заказчиком.
5. Составить перечень необходимого оборудования с учетом требований п. 4.
6. Составить перечень оборудования, учитывая требования п. 5, с возможным дублированием приборов.
7. Произвести расчет вероятностей отказа выбранных приборов с учетом результатов, полученных в п. 6
8. Построить ациклический граф возможной конфигурации системы.
9. Решить задачу определения кратчайших путей с учетом ограничений.

Для решения задачи можно использовать метод, с помощью которого задача решается кратчайшим путем, минимизировав целевую функцию. Она приобретет такой вид:

$$\min\left\{\sum_{i=1}^{N}\left|\log\left(1-x_i^{x_j^i}\right)\right|\right\}.$$

Выводы. Предложенные подходы к определению эффективности средств ЗИ следует использовать при создании системы ЗИ конкретного объекта. Причем эти критерии могут быть различными. Очевидно, что практически всегда в этих критериях будет присутствовать стоимость оборудования, обеспечивающего ЗИ, вероятность несанкционированного снятия информации, вероятность отказа систем ЗИ. В любом случае разработчикам системы придется сталкиваться с многокритериальной задачей, решение которой достаточно сложно.

В некоторых случаях при постановке задач могут возникнуть ограничения, например, на количество приборов, их вес, стоимость и т.д. Заданный

уровень безопасности следует обеспечивать набором приборов, которые перекрывают весь спектр возможных угроз как по каналам утечки информации, так и по ее искажению. Под искажением понимается нарушение целостности, т.е. как непосредственно искажение, так и полное или частичное уничтожение.

Следует отметить тот факт, что в своей совокупности комплекс приборов приобретает новые свойства, которые не свойственны каждому прибор в отдельности. Этот факт необходимо учитывать при выборе номенклатуры приборов, чтобы избежать дублирования и повышением стоимости системы.

Список литературы: 1. *Кравченко В.И.* Электромагнитное оружие / *Кравченко В.И.* – Харьков: НТУ «ХПИ», 2008. – 185 с. **2.** *Кравченко В.И.* Оружие на нетрадиционных принципах: Электромагнитное оружие / *Кравченко В.И.* – Харьков: НТУ «ХПИ», 2009. – 266 с**. 3.** ДСТУ 28-60-94**.** Надійність техніки**. –** К.: Держстандарт України**,** 1994**. –** 36 с. **4.** Новый энциклопедический словарь. –М.: Большая Российская энциклопедия, РИПОЛ Классик, 2004. – 1456 с. **5.** *Пєвнєв В.Я.* Эффективность информационной безопасности замкнутых систем / *Пєвнєв В.Я.* // Радіоелектронні і комп'ютерні системи. – Вип. 5(39). – Харьков «ХАИ», 2009. – С. 82-85. **6.** Серков А.А., Пєвнєв В.Я. Информационная безопасность: концепция и средства обеспечения // Вісник НТУ «ХПІ». Збірник наукових праць. Тем.вип: Техніка і електрофізика високих напруг. – Харьков: НТУ «ХПІ». – 2008. – № 44. – С. 132-136. **7.** *В.С. Харченко, Г.М. Тимонькін, В.О. Сичов, І.В. Лисенко* Теорія надійності та живучості елементів і систем літальних комплексів. – Харків 1997. – С. 13-14. **8.** ДСТУ 28-61-94. Державний стандарт України.

Поступила в редакцию 09.10.2009

УДК 622.24 : 537. 528

О.Н.СИЗОНЕНКО, докт.техн.наук, Институт импульсных процессов и технологий НАН Украины, Николаев;
Г.А.БАГЛЮК, докт.техн.наук, Институт проблем материаловедения им. И.М.Францевича НАН Украины, Киев;
А.И.РАЙЧЕНКО, докт.техн.наук, Институт проблем материаловедения им. И.М.Францевича НАН Украины, Киев;
А.И.ИВЛИЕВ, канд.техн.наук, Институт импульсных процессов и технологий НАН Украины, Николаев;
Е.В.ЛИПЯН, Институт импульсных процессов и технологий НАН Украины, Николаев

ВЛИЯНИЕ ВЫСОКОВОЛЬТНОГО ЭЛЕКТРИЧЕСКОГО РАЗРЯДА НА ИЗМЕНЕНИЕ КОМПОЗИЦИИ ПОВЕРХНОСТИ ДИСПЕРСНЫХ ПОРОШКОВ 60FE50TIC И СВОЙСТВ СПЕЧЕННЫХ МАТЕРИАЛОВ

Наведено результати експериментальних комплексних досліджень впливу обробки суспензії порошку 60Fe50TiC високовольтним електричним розрядом на властивості спечених матеріалів.