УДК 004.432

М.С. Политов, А.В. Мельников

Полная структурная оценка защищенности ИС

Сделана попытка найти наиболее эффективную методику и систему критериев для оценки уровня защищённости информационных систем. Был проведён анализ существующих и успешно применяющихся сегодня критериев с выявлением их преимуществ и проблемных аспектов. По результатам исследования была сформулирована и предложена новая система критериев оценивания уровня защищённости.

Введение

При планировании и развёртывании информационных систем перед специалистами ставится задача создания не просто системы, которая выполняла бы определённые функции, но и накладывается ряд существенных требований, таких как надёжность и сохранность, доверенных системе данных, эквивалентная стоимость которых часто превышает стоимость самой системы. На сегодня актуальность необходимости защиты информации неоспорима, т.е. любая спроектированная и сданная в эксплуатацию система должна нести в себе функции защиты и предотвращения несанкционированного доступа. Очевидно, что защита информации должна носить комплексный характер, но также необходимо учитывать и возможность возникновения (или невозникновения) угроз, специфичных для данной конкретной информационной системы. На этом этапе анализа важно не упустить существенных деталей и в то же время не переоценить некоторые из них, ибо это может повлечь неоправданные финансовые и материальные расходы на организацию системы предотвращения возникновения подобных ситуаций. Приступая к созданию системы информационной безопасности, необходимо оценить, какие угрозы наиболее актуальны.

Типовые подходы к анализу защищённости

В настоящее время, видимо, не существует каких-либо стандартизированных методик анализа защищенности АС, лишённых субъективного фактора. Поэтому в конкретных ситуациях алгоритмы действий аудиторов существенно различаются. Современные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную либо с использованием специализированных программных средств. Но здесь возникает проблема выбора и сравнения полученных результатов. Используя активные и пассивные методы тестирования, как по результатам оценить или сравнить уровни защищённости (уязвимости) разных конфигураций АС? Необходима некоторая абстрагированная от конкретных свойств системы шкала, в рамках которой и будет измеряться общий уровень безопасности. Как вариант предлагается использовать метод аналитической оценки и прогнозирования общего уровня защищённости, описанный в [1]. Данный метод позволяет оценить уровень защиты отдельных элементов АС.

Полное структурное оценивание систем

Любая АС состоит из множества подсистем, которые могут иметь абсолютно разные уровни защиты. Рассмотрим критерии и методы совокупной оценки, но прежде введём понятие уязвимости системы, комбинируя определения методик аудита безопасности и систем оценивания рисков.

• *Уязвимость любой системы* определяется уязвимостью значимых ресурсов этой системы.

Но что такое уязвимость или неуязвимость системы? Сказать, что эта система уязвима – значит ничего не сказать по сути, ибо нельзя, оценивая плотность вещества, назвать какое-то плотным, а какое-то нет. Уязвимость – понятие относительное.

Как правило, использование этого понятия отдельно сопряжено с рядом трудностей, поскольку всегда возникает логичный вопрос «Если уязвима, то насколько?». Поэтому оценка уровня уязвимости/защищённости будет более правильна и конкретна. Введём следующие определения и допущения:

1. Жизненный путь программно-технического средства будет оцениваться в количестве выпущенных производителем версий и модификаций.

2. Подсчёт количества версий ведётся не по числу реально используемых версий, а исходя из формальной системы образования порядкового номера версии. При этом не учитывается факт существования/отсутствия каждой отдельной.

3. Виды и типы уязвимостей классифицируем следующим образом:

• *Low* – уязвимости типа «поднятие локальных привилегий», но не до *local system*;

• *Midle* – уязвимости, мешающие нормальному функционированию системы и приводящие к возникновению *DoS*, уязвимости, приводящие к поднятию локальных привилегий до *local system*;

• *High* – уязвимости, позволяющие злоумышленнику получить удалённый контроль над системой.

4. Отношение уязвимостей определённого класса к количеству версий будет измеряться в поинтах. Один поинт будет характеризовать количество уязвимостей данного типа, приходящихся в среднем на одну версию программно-технического продукта.

Располагая эти оценки на единой шкале (в поинтах) и используя теорию временных рядов, можно прогнозировать уровень защищённости конкретной информационной системы с учётом её развития на ближайшее будущее.

Если система имеет несколько целевых узлов, то совокупная уязвимость рассчитывается следующим образом:

$$\text{СУИС}=\text{К}_1\text{ЧУИС}_1+\text{К}_2\text{ЧУИС}_2+\ldots+\text{К}_i\cdot\text{УИС}_i,$$

где i – порядковый номер информационной подсистемы; СУИС – совокупная уязвимость информационной системы; К_i – коэффициент долевого участия важности каждой конкретной системы в общей значимости всей ИТ-инфраструктуры. Измеряется в процентах.

Для оценки совокупной уязвимости информационной системы воспользуемся логическими схемами, представленными ниже.

I. Модель последовательного соединения звеньев системы:

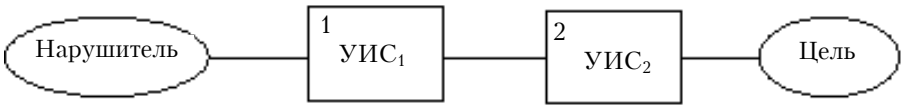

Рис. 1. Последовательная логическая схема «Нарушитель–Цель»

$$p(AB) = p(A)\cdot p(B) \quad (1)$$

II. Модель параллельного соединения звеньев системы:

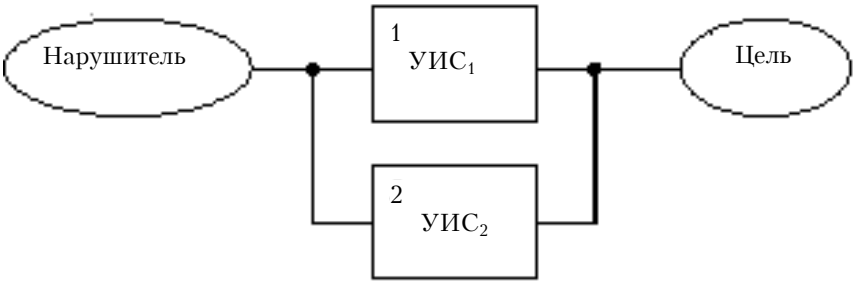

Рис. 2. Параллельная логическая схема «Нарушитель–Цель»

$$p(A + B) = p(A) + p(B) - p(A\cdot B) \quad (2)$$

III. Комбинированная схема соединения звеньев системы:

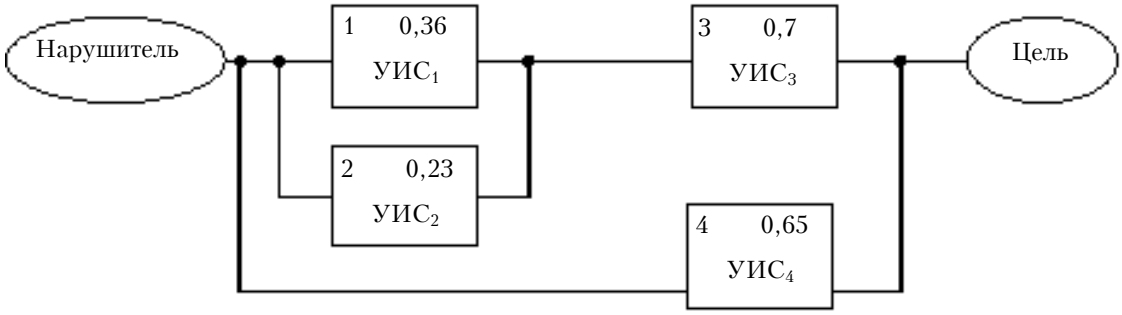

Рис. 3. Комбинированная логическая схема «Нарушитель–Цель»

Получаем формулу для совокупной уязвимости информационной системы:

$$\text{СУИС}=(\text{УИС}_1+\text{УИС}_2-\text{УИС}_1\text{ЧУИС}_2)\text{ЧУИС}_3+\text{УИС}_4-(\text{УИС}_1+\text{УИС}_2-\text{УИС}_1\text{ЧУИС}_2)\text{ЧУИС}_3\text{ЧУИС}_4, \quad (3)$$

$$\text{СУИС} = (0,36+0,23-0.36\cdot 0.23)\cdot 0,7+0,65-(0,36+0,23-0,36\cdot 0,23)\cdot 0,7\cdot 0,65 = 0,774\ .$$

Вывод

Использование теории временных рядов и предложенных выше метрики и полной структурной оценки систем позволяет прогнозировать уровень защищённости конкретной информационной системы с учётом её развития на ближайшее будущее. Ценность такой информации увеличивается благодаря тому, что получить её удаётся заранее (до того, как произойдёт плановое развитие информационной системы).

Литература

1. Information systems security analysis problems. Politov M.S. Computer Science and Information Technologies 2005, Volume 2, Ufa-USATU Editorial-Publishing Office
2. Complex System Vulnerability Estimation. Politov M.S. Computer Science and Information Technologies 2007, Volume 2, Ufa-USATU Editorial-Publishing Office
3. Филин С.А. Информационная безопасность. М.: Альфа-Пресс. 2006.
4. Common Criteria for Information Technology Security Evaluation. V. 1.0 31.01.96.

Политов М.С.

Мельников Андрей Витальевич
ГОУ ВПО «Челябинский государственный университет»
Проректор по научной работе, профессор, доктор технических наук
Эл. почта: mav@csu.ru.

M.S.Politov, A.V. Melnikov
Full structure security estimation system

This research makes attempt to find the most effective technique and system of criteria for an estimation of a security level of information systems. The analysis of criteria existing and successfully applied today with revealing their advantages and problem aspects has been lead. By research results the new system of criteria estimation a security level has been formulated and offered.