*В. О. Чутов*

# ФОРМАЛЬНАЯ ПОСТАНОВКА ЗАДАЧИ СОЗДАНИЯ РАЦИОНАЛЬНОГО ВАРИАНТА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУДИТА ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ

Проведенный системный анализ представленных на рынке систем (StatWin, Tivoli Configuration Manager, Tivoli Remote Control, OpenView Operations, Урядник/Enterprise Guard, Insider) позволил выделить ряд специфических свойств, придание которых перспективной АСАД позволит повысить ее показатели эффективности по сравнению с исследованными образцами.

В общем случае наряду с достаточно широким функционалом и большим пакетом опций были выявлены следующие основные слабые места:

- обязательное циклическое сканирование всех заданных элементов информационно-вычислительных систем (ИВС) (и в первую очередь АРМ пользователей);
- серьезные ограничения по оперативности и точности принимаемых решений, вызываемые человеческим фактором;
- сокращение возможностей ИВС по решению задач, для которых она предназначена, путем отбора вычислительного ресурса для нужд системы информационной безопасности (ИБ);
- сложность автоматизации адаптации к новой сетевой инфраструктуре в случае ее изменения.

Из приведенных результатов анализа следует очевидная необходимость придания перспективным мониторинговым системам *следующих свойств*:

- *автоматизации*, исключающей рутинные «ручные» операции;
- *сочетания централизации* (на базе автоматизированного рабочего места администратора безопасности) *с управлением на уровне отдельных элементов* (интеллектуальных компьютерных программ) системы аудита работы пользователей ИВС;
- *масштабируемости*, позволяющей проводить наращивание мощностей мониторинговых систем и расширение их возможностей без значительного увеличения вычислительных ресурсов, необходимых для их эффективного функционирования;
- *адаптивности* к изменению состава и характеристик ИВС, а также к появлению новых видов нарушений политики безопасности.

Для математического описания постановки задачи введем с помощью вектора $X(t)$ понятие состояния ИВС, под которым будем понимать совокупность всех обеспечиваемых ее возможностями действий пользователей:

$$X(t) = \{x_i(t)\},\ i = 1, 2, ..., i = 1, 2, ..., n \quad (1.1),$$

где время $t$ может быть как дискретным, так и непрерывным.

Обозначим через

$$X^n(t) = \{x_j^H(t)\},\ j = 1, 2, ..., n^n \quad (1.2)$$

подмножество всех несанкционированных действий пользователей (как авторизованных, так и неавторизованных), нарушающих политику безопасности и существенных с точки зрения обеспечения ИБ ИВС.

Будем предполагать, что имеется возможность с использованием той или иной прогнозирующей модели $M = \{Q \cup F\}$ (эвристической, математической) через некоторые операторы приведения $Q$ и $F$ оценить влияние несанкционированных действий $X^н(t)$ через соответствующие потери $\Delta\Pi(t)$ параметров $\Pi(t) = \{$целостность, доступность, конфиденциальность$\}$ информации на множество R значений рисков в деятельности ИВС, упорядоченное отношением $\geq$:

$$Q: X_H(t) \times \Omega_Q \rightarrow \Delta\Pi(t) \quad (1.3)$$

$$F: \Delta\Pi(t) \times \Omega_F \rightarrow R \quad (1.4),$$

где $\Omega_Q$ и $\Omega_F$ — соответственно множество неопределенностей, сопровождающих процесс приведения $Q$ и реализацию оценочного соотношения $F$.

Функционирование АСАД ИВС в условиях случайных и неслучайных возмущений $\Omega_Ф$ может быть представлено оператором $Ф$:

$$Ф: X_H(t) \times \Omega_Ф \rightarrow X_H(t) = \{X^{H1}(t) \cup X^{H2}(t)\}, \quad (1.5)$$

где $\widehat{X}^{н}(t)$ — оценка вектора $X^{н}(t)$, в общем случае отличающаяся от него вследствие наличия возмущений $\Omega_Ф$,

$X^{H1}(t) = \{x_{j1}^{H1}(t)\} \subset X(t)$, $j1 = 1, 2, ..., n_{H1}$ — наблюдаемые компоненты подмножества $X^{н}(t)$,

$X^{H2}(t) = \{x_{j1}^{H2}(t)\} \subset X(t)$, $j1 = 1, 2, ..., n_{H2}$ — вычисляемые компоненты подмножества $X^{н}(t)$.

Создание АСАД ИВС, как уже отмечалось выше, в конечном итоге направлено на обеспечение целостности, доступности и конфиденциальности обрабатываемой в ИВС информации. Собственник ИВС обладает возможностью проведения некоторых управляющих воздействий с использованием методов принятия решений в нештатных ситуациях:

$$U(t) = \{u_l(t)\}, \; l = 1, 2, ..., L. \quad (1.6)$$

Следует заметить, что условия физической реализуемости технических систем предполагают непременное наличие в общем случае зависящей от времени области ограничений $O^U$ на вектор управления $U(t)$:

$$U(t) \in O^U(t) \quad (1.7)$$

Представим подлежащие выбору и обоснованию характеристики АСАД ИВС как элемента подсистемы информационной безопасности ИВС некоторым вектором Y, в общем случае также зависящим от времени:

$$Y(t) = \{y_m(t)\}, \; m = 1, 2, ..., M. \quad (1.8)$$

В качестве его составляющих будут выступать характеристики структуры и состава АСАД ИВС, серверов, рабочих станций и коммуникационного оборудования, операционных систем и приложений, пользователей, подсистемы управления функционированием и т. д.

Так же как и в случае с вектором управления, необходимо предусмотреть наличие ограничений $O^Y(t)$ на ресурсные (аппаратно-программные, материальные, трудовые) затраты $З(t)$, направленные на реализацию того или иного варианта АСАД ИВС:

$$З(t) \subset O^Y(t) \quad (1.9)$$

Существующая в настоящее время идеология защиты информации в ИВС требует поиска компромисса, с одной стороны, между требованием обеспечения высокой эффективности выполнения тех задач, для которых предназначена данная ИВС, при максимальном удобстве работы пользователей, во многом определяемым ее открытостью, и, с другой стороны, требованием обеспечения ее информационной безопасности, определяемым максимальной закрытостью ее ресурсов и ограничением доступа к ним. Указанный компромисс обеспечивается созданием «дополнительных» аппаратно-программных средств защиты информации. Однако эти средства отбирают у ИВС необходимый для ее функционирования ресурс и увеличивают нагрузку на сеть. Чем выше устанавливаемый уровень информационной безопасности, тем больше требуется дополнительного вычислительного и сетевого ресурса для его обеспечения.

Задача выбора наилучшего в некотором смысле значения $Y(t)$ в соответствии с теорией исследования операций может быть решена путем максимизации эффективности управляющих воздействий $U(t)$ на основе информации $\widehat{X}^{н}(t) = \{X^{н1}(t) \cup X^{н2}(t)\}$ (результат возмущающего воздействия, где $X^{н1}$, $X^{н2}$ — наблюдаемые и вычисляемые множества соответственно), $\Delta П(t)$, R при выполнении ограничений (1.7) и (1.9) или минимизации затрат ресурсов $З(t)$ на создание АСАД ИВС при заданной величине эффективности управляющих воздействий (1.7).

Из приведенной выше математической постановки задачи следует, что для строгой оптимизации характеристик АСАД ИВС необходимо, прежде всего, формальное описание оценочного соотношения (1.4).

Указанное описание применительно к такой сложной системе, какой является ИВС, весьма затруднительно (если вообще возможно) в связи с многокритериальностью и большой размерностью задачи (как минимум, три показателя качества информации, большая размерность векторов $X(t)$ и $Y(t)$), с наличием большого количества неопределенностей ($\Omega_Q$, $\Omega_F$ и $\Omega_Ф$).

В связи с этим постановка задачи создания оптимальной в строгом математическом смысле АСАД ИВС (обеспечения абсолютной защиты информации от несанкционированных действий пользователей) практически не представляется возможной. Реализуемой может быть лишь задача об относительной защищенности ИВС, т. е. о максимально возможном приближении к желаемому состоянию параметров целостности, доступности и конфиденциальности циркулирующей в ней информации.

Другими словами, речь может идти о сохранении рисков от изменения этих параметров в некоторых заранее заданных пределах r, т. е. о создании рациональной в указанном смысле АСАД ИВС.

Таким образом, рациональными характеристиками АСАД ИВС на некотором временном интервале T с учетом выражений (1.3) и (1.4) могут считаться характеристики:

$$Y^{рац}(t) = \{Y_m^{рац}(t)\},\ m = 1, 2, ..., M \quad (1.10),$$

значения которых при реализации неопределенностей:

$$q_Q \in \Omega_Q,\ q_F \in \Omega_F,\ q_Ф \in \Omega_Ф,$$

$$F_j\{Y^{рац}(t), X^H(t), U(t), Э(t)\} \le rj, \quad (1.11)$$

$$U(t) \in O^U(t)$$

$$Э(t) \subset O^Y(t)$$

$$r \in R$$

$$t \in T$$

$$j = 1, 2, ..., n_H$$

## СПИСОК ЛИТЕРАТУРЫ:

1. *Вентцель Е. С.* Исследование операций. М.: Сов. Радио, 1972.
2. *Вагнер Г.* Основы исследования операций. М.: Мир, 1973.
3. *Красноступ Н. Д., Кудин Д. В.* Шпионские программы и методы защиты от них. URL: http://bezpeka.com/library/adm/spy-v-antispy.htm.
4. Spector Pro 5.0. 2004. URL: http://www.spectorsoft.com.
5. PC Activity Monitor Series. Raytown Corporation LLC. 2004. URL: http://www.softsecurity.com/index.htm.
6. СОВА РС. ООО «Центр информационной безопасности». Запорожье, 2004. URL: http://www.bezpeka.biz.
7. SpyAgent 5.1. 2004. URL: http://www.spytech-web.com.
8. HSLAB Logger. Handy Software Lab. 2004. URL: http://www.hs-lab.com/rus/products/logger/index.htm.
9. Урядник (Enterprise Guard). URL: http://rnt.ru.