

## ВЫБОР МЕТОДОВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПО КРИТЕРИЮ ЭФФЕКТИВНОСТИ

к.т.н. С.В. Арепьев, к.ф.-м.н. А.А. Можаяев, к.т.н. В.А. Гирдвоин  
(представил д.т.н., проф. А.И. Стрелков)

Предложен подход к решению задачи выбора метода технической защиты информации по критерию эффективности с учетом конкретных условий обстановки при отсутствии априорных данных о применяемых методах несанкционированного доступа к информации.

В настоящее время во всех областях жизни и деятельности нашего общества наблюдается бурный рост случаев негласного получения информации с использованием технических средств. При этом уровень развития самих технических средств негласного получения информации, а также методов их применения, достиг такого уровня, что осуществлять защиту от таких злонамеренных действий становится все труднее и труднее. Современные методы и средства негласного получения информации позволяют фиксировать информационные сигналы (как акустические, так и электромагнитные) не только без предварительного размещения специальных средств в интересующих помещениях, но и на значительном удалении от них.

Из сказанного выше можно сделать вывод, что осуществление защиты информации от несанкционированного доступа за счет применения технических средств является одной из наиболее актуальных задач. В настоящее время разработано достаточное количество методов технической защиты информации, а также постоянно разрабатываются новые. В данных условиях существует проблема выбора метода технической защиты информации, который обеспечивал бы наиболее эффективную защиту с учетом конкретных условий обстановки.

В общем случае работы по технической защите информации (ТЗИ) состоят из организационных, подготовительных технических, технических мероприятий и контроля за выполнением мер технической защиты информации и за эффективностью этой защиты. Организационные и подготовительные технические мероприятия по технической защите информации проводятся одновременно и являются первым этапом работ, технические мероприятия - последующим этапом работ. Мероприятия по ТЗИ и контролю за её эффективностью выполняются постоянно в процессе эксплуатации технических средств защиты информации.

Остановимся на организационных мероприятиях по технической

защите информации, так как они являются одним из главных факторов, определяющих эффективность этой защиты.

В общем случае организационные мероприятия по защите информации подразделяются на следующие основные этапы:

- выявление возможных каналов утечки информации путем обследования выделенных помещений и прилегающих территорий;
- выбор наиболее эффективных методов защиты информации на основе результатов анализа возможных каналов утечки информации;
- определение необходимого состава технических средств для реализации выбранных методов защиты информации.

Опыт показывает, что задача выявления возможных каналов утечки информации у специалистов затруднений не вызывает. Гораздо более сложной является задача выбора наиболее эффективных методов защиты информации применительно к конкретным условиям обстановки. Рассмотрим данную задачу более подробно.

Исходными данными для решения задачи выбора наиболее эффективных методов защиты информации являются:

- требуемый гарантированный уровень защиты информации;
- множество возможных методов несанкционированного доступа к информации для данного канала утечки информации;
- множество возможных методов защиты информации для данного канала утечки информации.

Предположим, что в конкретном случае имеется множество возможных методов несанкционированного доступа к информации  $\mathbf{A}$  и множество возможных методов защиты информации  $\mathbf{B}$ , а также требуемый гарантированный уровень защиты информации  $y_{\text{тр}}$ . Таким образом, на уровень защиты информации  $y$  влияет не только выбор метода  $\mathbf{v} \in \mathbf{B}$ , но и применение противником метода  $\mathbf{a} \in \mathbf{A}$ , т.е.  $y(\mathbf{a}, \mathbf{v})$ . Следовательно, функция соответствия будет измерять степень соответствия реального уровня защиты информации требуемому, т.е.

$$\rho = \rho(y(\mathbf{a}, \mathbf{v}), y_{\text{тр}}) . \quad (1)$$

В данной ситуации, как показано в [1], необходимо ввести математическое ожидание функции соответствия (условный показатель эффективности):

$$\mathbf{W}(\mathbf{a}, \mathbf{v}) = \mathbf{M}[\rho(y(\mathbf{a}, \mathbf{v}), y_{\text{тр}})] . \quad (2)$$

Кроме того, по вполне понятным причинам, можно предположить, что противник будет выбирать такие методы  $\mathbf{a} \in \mathbf{A}$ , которые позволяли бы при использовании любого метода  $\mathbf{v} \in \mathbf{B}$  минимизировать степень соответствия реального уровня защиты информации требуемому. Таким образом, в этих условиях в качестве показателя эффективности наиболее

целесообразно выбирать минимальное значение  $W(\mathbf{a}, \mathbf{b})$  для каждого метода  $\mathbf{a} \in \mathbf{A}$ :

$$W(\mathbf{b}) = \min_{\mathbf{a} \in \mathbf{A}} M[\rho(\mathbf{y}(\mathbf{a}, \mathbf{b}), \mathbf{y}_{\text{тп}})] . \quad (3)$$

Таким образом, показатель (3) является гарантированным уровнем защиты информации, т.е. позволяет гарантировать уровень показателя (2). Другими словами при использовании любого метода несанкционированного доступа к информации и применении конкретного метода защиты информации показатель (3) является нижней границей математического ожидания функции соответствия реального уровня защиты информации требуемому.

Анализ сказанного выше позволяет сделать вывод о том, что в качестве критерия эффективности методов защиты информации следует выбирать критерий наибольшего гарантированного результата [1]. Смысл данного критерия заключается в том, что при случайном характере результата  $\mathbf{y}(\mathbf{b})$  использования какого-то определенного метода защиты информации, гарантированным результатом (вероятностно - гарантированным результатом) является уровень  $\mathbf{y}_{\delta}(\mathbf{b})$ , не ниже которого будет получен реальный результат с заданной вероятностью, т.е.

$$\delta = P(\mathbf{y}(\mathbf{b}) \geq \mathbf{y}_{\delta}(\mathbf{b})) . \quad (4)$$

С учетом того, что показателем эффективности является выражение (3), а критерием эффективности является критерий наибольшего гарантированного результата, можно определить оптимальное условие для выбора метода защиты информации

$$\mathbf{b}^* = \max_{\mathbf{b} \in \mathbf{B}} \min_{\mathbf{a} \in \mathbf{A}} M[\rho(\mathbf{y}(\mathbf{a}, \mathbf{b}), \mathbf{y}_{\text{тп}})] . \quad (5)$$

Выбор метода технической защиты информации путем использования выражения (5) позволяет максимизировать уровень защиты информации и минимизировать возможности любого метода несанкционированного получения информации

В [1] показано, что критерий наибольшего гарантированного результата является оптимальным при высоких уровнях степени гарантии ( $\delta > 0,6 \div 0,7$ ) результата.

На рис.1 (по аналогии со схемой, описанной в [1]) представлена схема выбора метода защиты информации по критерию наибольшего гарантированного результата. Так, например, для случая, когда из двух возможных методов  $\mathbf{b}_1$  и  $\mathbf{b}_2$  по уровню вероятностной гарантии  $\delta$  предпочтение отдается методу  $\mathbf{b}_2$  ввиду того, что  $\mathbf{y}_{\delta}(\mathbf{b}_1) < \mathbf{y}_{\delta}(\mathbf{b}_2)$ .

Изложенное выше позволяет сделать следующие выводы:

- в случае выбора наиболее эффективного метода защиты информации для известного канала утечки информации в условиях отсутствия

априорных данных о применяемых методах несанкционированного доступа к информации, критерий наибольшего гарантированного результата является наиболее оптимальным;

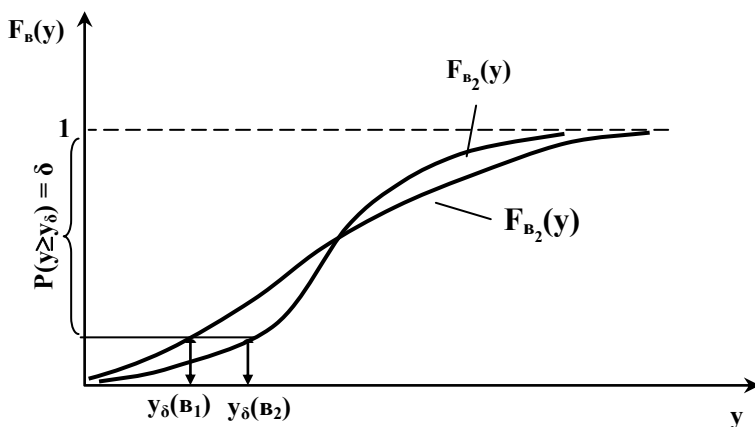


Рис. 1. Схема выбора метода защиты информации по критерию наибольшего гарантированного результата

- критерий наибольшего гарантированного результата позволяет получить уровень защиты информации не ниже требуемого, что особенно важно в быстро меняющихся условиях обстановки;
- описанный выше подход к решению задачи выбора метода технической защиты информации позволяет минимизировать ущерб от действий враждебной стороны.

## ЛИТЕРАТУРА

1. Надежность и эффективность в технике. Справочник в десяти томах. Том 3 / Под ред. В.Ф. Уткина. – М.: Машиностроение, 1988. – 328 с.

*Поступила в редколлегию 2.07.2001*