УДК 621.371

ВЫБОР МЕТОДОВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПО КРИТЕРИЮ ЭФФЕКТИВНОСТИ

к.т.н. С.В. Арепьев, к.ф-м.н. А.А. Можаев, 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 использование 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 интересуемых 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 зашиты информации для данного канала утечки информации.

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

$$\rho = \rho(\mathbf{y(a,в)}, \mathbf{y_{тр}}) \ . \qquad (1)$$

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

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

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

целесообразно выбирать минимальное значение **W(а,в)** для каждого метода **а∈А**:

$$W(в) = \min_{а \in A} M\,[\,\rho(y(a,в), y_{тр}\,]\,. \qquad (3)$$

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 **y(в)** использования какого-то определенного метода защиты информации, гарантированным результатом (вероятностно - гарантированным результатом) является уровень $y_{\delta}(в)$, не ниже которого будет получен реальный результат с заданной вероятностью, т.е.

$$\delta = P(y(в) \geq y_{\delta}(в))\,. \qquad (4)$$

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

$$в^{*} = \max_{в \in B} \min_{а \in A} M[\rho(y(a,в), y_{тр}\,]\,. \qquad (5)$$

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 $в_1$ и $в_2$ по уровню вероятностной гарантии δ предпочтение отдается методу $в_2$ ввиду того, что $y_{\delta}(в_1) < y_{\delta}(в_2)$.

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;

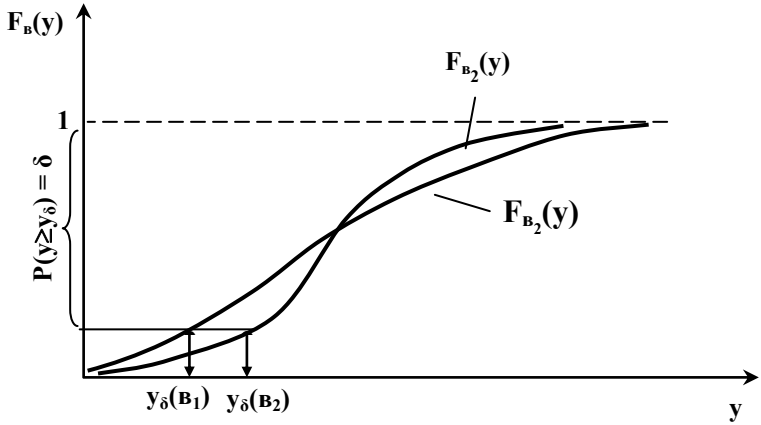

Рис. 1. Схема выбора метода защиты информации по критерию наибольшего гарантированного результата

– 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