УДК 621.371

ВЫБОР МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ПО КРИТЕРИЮ ЭФФЕКТИВНОСТИ ПРИ ОТСУТСТВИИ АПРИОРНЫХ ДАННЫХ О ПРОТИВОБОРСТВУЮЩЕЙ СТОРОНЕ И НАЛИЧИИ РЕСУРСНО-ВРЕМЕННЫХ ОГРАНИЧЕНИЙ

к.т.н. С.В. Арепьев
(представил д.т.н., проф. Д.В. Голкин)

Предложен подход к решению задачи выбора метода защиты информации по критерию эффективности при отсутствии априорных данных о противоборствующей стороне и наличии ресурсно-временных ограничений на организацию технической защиты информации.

Постановка проблемы. Широчайшее повсеместное внедрение во все сферы жизнедеятельности современного общества технических средств передачи, обработки и хранения информации (ТСПИ) создает благоприятные условия для осуществления несанкционированного доступа к конфиденциальной информации ввиду низкой защищенности данных средств с одной стороны и низким уровнем организации технической защиты информации – с другой. Эффективность технической защиты информации (ТЗИ) главным образом зависит от квалификации лица, занимающегося организацией ТЗИ (ЛОТЗИ). При этом основной трудностью, с которой сталкивается ЛОТЗИ в процессе своей деятельности, является адекватный выбор методов ТЗИ (МТЗИ) из всего их многообразия, применительно к конкретным условиям обстановки. Анализ существующих рекомендаций по организации ТЗИ показывает, что они не всегда отвечают требованиям оперативности в условиях наличия временных ограничений на организацию ТЗИ, а также не учитывают возможное наличие ресурсных ограничений, что, в свою очередь, затрудняет ЛОТЗИ процесс выбора методов ТЗИ с точки зрения их пригодности в данной ситуации. Поэтому разработка рекомендаций по организации ТЗИ в условиях наличия ресурсно-временных ограничений является важной научно-технической задачей.

Анализ литературы. В работе [1] предложен подход к решению задачи выбора МТЗИ при условии отсутствия априорных данных о противоборствующей стороне (ПС) и отсутствии ресурсно-временных ограничений на организацию ТЗИ. Анализ данного подхода показывает, что

при условии наличия ресурсно-временных ограничений на организацию ТЗИ выбранные путем его использования МТЗИ могут не отвечать требованиям оперативности и их применение может оказаться невозможным ввиду наличия ограниченного количества ресурсов. Данный факт, в конечном итоге, может привести к тому, что задача организации ТЗИ в пределах установленных сроков может быть не выполнена. Другой подход к выбору МТЗИ, описанный в работе [2], предполагает наличие априорных данных о ПС. Однако такое условие не всегда выполнимо на практике. Кроме того, данный подход также не учитывает возможные ресурсно-временные ограничения на организацию ТЗИ. Таким образом оба этих подхода могут быть неприемлемы для решения задачи выбора МТЗИ в условиях ресурсно-временных ограничений на организацию ТЗИ и отсутствия априорных данных о ПС.

Цель статьи. В данной работе рассматривается предлагаемый автором подход к решению задачи выбора МТЗИ в условиях наличия ресурсно-временных ограничений на организацию ТЗИ и отсутствия априорных данных о противоборствующей стороне.

Рассмотрим описанный выше случай более подробно. Допустим, что имеются в наличии следующие начальные условия:

– определен технический канал утечки информации (ТКУИ);

– проведена оценка возможности организации негласного доступа к информации (применительно к данному ТКУИ) за счет использования известных технических методов негласного доступа к информации, с учетом временного периода от момента принятия решения о месте и времени проведения конфиденциального мероприятия до момента окончания данного мероприятия;

– имеется совокупность МТЗИ, при использовании которых возможно решение задачи закрытия данного ТКУИ;

– существуют ресурсные ограничения на организацию ТЗИ;

– существуют временные ограничения на организацию ТЗИ;

– априорные данные о ПС отсутствуют.

Перед ЛОТЗИ стоит задача выбора МТЗИ из имеющейся совокупности, который бы отвечал следующим требованиям:

– время реализации выбранного МТЗИ должно соответствовать существующим временным ограничениям на организацию ТЗИ;

– количество ресурсов, необходимое для реализации выбранного МТЗИ, должно соответствовать существующим ресурсным ограничениям на организацию ТЗИ;

– выбранный МТЗИ должен обеспечивать необходимый уровень защиты информации.

Следует отметить, что ситуация, когда на организацию ТЗИ накладываются ресурсно-временные ограничения, на практике возникает обычно тогда, когда появляется необходимость проведения конфиденциальных мероприятий в необорудованных для этой цели местах и на определенный временной период [3]. В данном случае требуемый результат мероприятий по ТЗИ обычно носит случайный характер, т.е. требуемый уровень защиты информации должен быть обеспечен только на срок, отведенный на проведение конфиденциальных мероприятий. Из изложенного следует, что в качестве показателя эффективности может быть принят уровень защиты информации, получаемый с заданной вероятностью.

Допустим, что для рассматриваемого ТКУИ существует совокупность U методов ТЗИ и необходимо осуществить выбор наиболее рационального МТЗИ $u \in U$, который позволит обеспечить уровень защиты информации $\tilde{y}(u)$ (имеющий случайный характер), с вероятностью α и функцией распределения $F(y_\alpha)$, тогда вероятность α (по аналогии с [4]) можно описать выражением

$$\alpha = P(\tilde{y}(u) \geq y_\alpha) \qquad (1)$$

или

$$\alpha = 1 - F(y_\alpha), \qquad (2)$$

где y_α – требуемый уровень защиты информации, получаемый с вероятностью α.

Тогда функция соответствия достигаемого уровня защиты информации требуемому будет определяться выражением (по аналогии с [5]):

$$\rho = F^{-1}(1-\alpha), \qquad (3)$$

а показатель эффективности, при условии, что ρ есть величина неслучайная и ее математическое ожидание равно ρ, будет иметь вид

$$W(u) = M[\rho] = y_\alpha, \qquad (4)$$

который обычно называют вероятностно-гарантированным результатом [3], или, в нашем случае, вероятностно-гарантированным уровнем технической защиты информации.

Исходя из условий поставленной задачи, можно сделать вывод, что существующее множество МТЗИ для данного канала ТКУИ можно разделить на два подмножества: $U_{пр}$ – множество МТЗИ, применение которых позволит уложиться в рамки накладываемых ресурсно-временных ограничений (т.е. множество пригодных МТЗИ) и множество $U \setminus U_{пр}$ МТЗИ, при применении которых ресурсно-временные затраты на орга-

низацию ТЗИ выйдут за рамки существующих ограничений (т.е. подмножество неприемлемых МТЗИ). Отсюда следует, что в качестве концепции рационального поведения при данных условиях следует применять концепцию пригодности [3], согласно которой, а также в соответствии с выражениями (1 – 4), критерий выбора МТЗИ можно определить как

$$u^* : y_\alpha(u) \geq y_{тр}, \qquad (5)$$

где $y_{тр}$ – допустимый гарантированный (с вероятностью α) уровень закрытия рассматриваемого ТКУИ.

Выводы. Предложенный в данной работе подход к решению задачи выбора МТЗИ позволяет:

– повысить оперативность мероприятий по организации ТЗИ;

– достигать требуемый уровень технической защиты информации на определенный период, в условиях наличия ресурсно-временных ограничений на организацию ТЗИ;

– осуществлять выработку рационального решения на организацию ТЗИ в условиях отсутствия априорных данных о противоборствующей стороне.

ЛИТЕРАТУРА

1. *Арепьев С.В., Можаев А.А., Гирдвоин В.А. Выбор методов защиты информации по критерию эффективности // Системи обробки інформації. – Х.: НАНУ, ПАНМ, ХВУ. – 2001. – Вип. 4(14). – С. 200 – 203.*
2. *Арепьев С.В. Выбор методов защиты информации по критерию эффективности при наличии априорных данных о противоборствующей стороне // Системи обробки інформації. – Х.: ХВУ. – 2003. – Вип. 5. – С. 192 –195.*
3. *Домарёв В.В. Безопасность информационных технологий. Методология создания систем защиты. – М.-С.Пб.-К.: Диасофт, 2002. – 688 с.*
4. *Анохин А.М., Глотов В.А., Павельев В.В., Черкашин А.М. Методы определения коэффициентов надежности критерия // Автоматика и телемеханика. – 1997. – № 8. – С. 3 – 35.*
5. *Надежность и эффективность в технике. Справочник в десяти томах. Т. 3 / Под ред. В.Ф. Уткина. – М.: Машиностроение, 1988. – 328 с.*

Поступила 26.12.2003

***АРЕПЬЕВ Сергей Викторович**, канд. техн. наук, начальник НИЛ научного центра при Харьковском военном университете. В 1993 году окончил Харьковское ВВКИУ РВ. Область научных интересов – техническая защита информации.*