УДК 681.3.067

ОПТИМИЗАЦИЯ СОСТАВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЕ С КАНАЛАМИ БЕСПРОВОДНОГО ДОСТУПА НА ОСНОВЕ ГРАФА РЕАЛИЗАЦИИ УГРОЗ

Г. Н. Мальцев,
доктор техн. наук, профессор
Военно-космическая академия им. А. Ф. Можайского
В. В. Теличко,
зам. директора
ООО «Цифровые технологии»

Приводится описание теоретико-множественной постановки и графового метода решения задачи выбора оптимального состава комплекса средств защиты информации распределенной информационно-управляющей системы с каналами беспроводного доступа. Рассмотрены особенности составления и преобразования графов реализации угроз в системах с каналами беспроводного доступа, для которых характерна возможность достижения нарушителем своих целей при реализации различного числа угроз и при различных последовательностях их реализации.

В современных информационно-управляющих системах (ИУС) дистанционного управления транспортными средствами и территориально разнесенными производственными процессами, сбора информации и удаленного доступа для информационного обмена между центральными и периферийными терминалами широкое распространение получают цифровые технологии передачи данных, которые реализуются как на основе кабельных сетей связи, так и с помощью систем беспроводного доступа [1, 2]. Технологии беспроводных сетей привлекают внимание разработчиков телекоммуникационных систем относительно невысокими экономическими затратами и простотой развертывания, удобством использования и гибкой архитектурой.

Практический интерес представляет использование в распределенных ИУС трех стандартизованных технологий беспроводного доступа: VPAN (Bluetooth, стандарт IEEE 802.15), WLAN (Wi-Fi, стандарт IEEE 802.11) и WMAN (Wi-MAX, стандарт IEEE 802.16). Их дальность действия изменяется от десятков и сотен метров (технологии VPAN и WLAN) до единиц километров (технология WMAN), а скорости передачи данных — от сотен килобит в секунду (технология VPAN) до десятков и сотен мегабит в секунду (технологии WLAN и WMAN). Однако сам принцип беспроводной передачи данных по радиоканалам, связывающим удаленные терминалы с точками входа в стационарную сеть, заключает в себе возможность несанкционированных подключений к точкам доступа, и развитие систем беспроводного доступа сопровождается усилением активности нарушителей, использующих уязвимости в построении систем передачи данных для реализации угроз информационной безопасности [3, 4].

В результате использование в распределенных ИУС каналов беспроводного доступа приводит к увеличению угроз информационной безопасности и необходимости принятия упреждающих мер по обеспечению требуемого уровня безопасности информации, циркулирующей в сети, и сведению к минимуму возможного ущерба от действий потенциальных нарушителей. Без обеспечения информационной безопасности ни повышение скоростей передачи данных, ни расширение спектра предоставляемых услуг, ни улучшение качества связи не смогут гарантировать эффективное функционирование самого высокотехнологичного оборудования. Таким образом, информационная безопасность сетей беспроводного доступа является важным условием существования и развития этой технологии, а также ее эффективного использования при решении прикладных задач.

Требуемый уровень безопасности информации в ИУС обеспечивается созданием и поддержанием в работоспособном состоянии комплекса аппаратно-программных средств защиты информации.

Состав комплекса средств защиты информации ИУС определяется, исходя из требований к информационной безопасности системы, ожидаемых угроз и целей нарушителей. Использование технологий беспроводного доступа усложняет задачу обеспечения информационной безопасности ИУС и выбора состава комплекса средств защиты вследствие увеличения числа угроз и различных вариантов их реализации при несанкционированном доступе к ИУС по радиоканалам. При этом механизмы обеспечения безопасности и частные аппаратно-программные решения, относящиеся к отдельным технологиям и каналам беспроводного доступа [2], выступают в качестве элементов множества средств защиты, которые следует принимать во внимание при оптимизации или рациональном выборе состава комплекса средств защиты. В настоящей работе развивается один из подходов к оптимизации состава средств защиты информации в распределенных информационных системах, основанный на составлении и анализе графа реализации ожидаемых угроз.

Формализованная теоретико-множественная постановка задачи синтеза оптимального состава комплекса средств защиты информации состоит в следующем [5]. Задаются множества угроз информации $\mathrm{A} = \{A_1, A_2, ..., A_M\}$ и целей нарушителя $\mathrm{B} = \{B_1, B_2, ..., B_F\}$. Полагается, что достижение f-й цели нарушителя B_f включает реализацию множества угроз $\mathrm{A}^f = \left\{A_1^f, A_2^f, ..., A_{M_f}^f\right\}$, где $f = 1, 2, ..., F$, $\mathrm{A}^f \in \mathrm{A}$. Для противодействия угрозам выбираются средства защиты информации из множества $\mathrm{Z} = \{Z_1, Z_2, ..., Z_N\}$, при этом для противодействия m-й угрозе информации формируется m-й рубеж защиты, на котором используются средства защиты из множества $\mathrm{Z}_m^f = \left\{Z_{m1}^f, Z_{m2}^f, ..., Z_{mN_f}^f\right\}$, где $m = 1, 2, ..., M$, $\mathrm{Z}_m^f \in \mathrm{Z}$. Для множеств угроз A и средств защиты Z выполняются следующие отношения:

$$\bigcup_{f=1}^{F} \mathrm{A}^f = \mathrm{A} \text{ и } \bigcup_{f=1}^{F} \bigcup_{m=1}^{M_f} \mathrm{Z}_m^f = \mathrm{Z}.$$

Необходимо найти матрицы использования средств защиты Z_m^f на M_f рубежах защиты при противодействии f-й цели нарушителя:

$$\mathbf{X}^f = \begin{bmatrix} x_{11}^f & \dots & x_{1N_f}^f \\ \dots & \dots & \dots \\ x_{M_f1}^f & \dots & x_{M_fN_f}^f \end{bmatrix}, \qquad (1)$$

где $x_{mn}^f = \begin{cases} 1, \text{ если } n\text{-е средство используется} \\ \text{на } m\text{-м рубеже защиты;} \\ 0, \text{ если } n\text{-е средство не используется} \\ \text{на } m\text{-м рубеже защиты,} \end{cases}$

обеспечивающие выполнение условия

$$\mathbf{X}_{\text{opt}}^f \to \max_{x_{mn}^f} \prod_{f=1}^{F} \left[1 - \sum_{m=1}^{M_f} \prod_{n=1}^{N_f} \left(1 - P_{mn}^f x_{mn}^f \right) \right], \qquad (2)$$

где P_{mn}^f — вероятность успешного функционирования n-го средства на m-м рубеже защиты. Условие (2) определяет критерий оптимальности — максимум вероятности успешного противодействия комплекса средств защиты всем целям нарушителя. Исходя из данного критерия осуществляем решение задачи. Совокупность матриц использования средств защиты $\mathbf{X}_{\text{opt}}^f$, $f = 1, 2, ..., F$, вида (1), найденных в результате решения задачи оптимизации (2), определяет оптимальный состав средств защиты из множества Z для заданных множеств угроз A и целей нарушителя B.

Приведенная формализованная постановка оптимизационной задачи позволяет, с одной стороны, учесть многообразие угроз информации и вариантов их реализации (целей нарушителя), с другой стороны, согласовать полученное решение с заданным профилем защиты информации ИУС. Профиль защиты информации представляет собой независимую от реализации совокупность требований безопасности для некоторой категории информационных систем (в рассматриваемом случае — ИУС), отвечающую специфическим запросам потребителя. Порядок формирования профиля защиты информации, исходя из требований безопасности, целей безопасности и свойств среды безопасности, определяется ГОСТ Р ИСО/МЭК 15408–2001 [6], основные требования которого в рассмотренной формализации угроз информационной безопасности и средств их предотвращения могут быть учтены. В частности, множество угроз безопасности определяется целями безопасности, множество целей нарушителя определяется средой безопасности, а найденный состав средств оптимального профиля защиты должен отвечать соответствующим требованиям безопасности.

В качестве ограничений при оптимизации состава средств защиты информации могут использоваться ограничения по общей стоимости комплекса средств защиты, по вероятностям противодействия комплекса средств защиты отдельным целям нарушителя, по риску достижения нарушителем своих целей. При этом ограничения по вероятностям противодействия отдельным целям нарушителя и по риску достижения нарушителем своих целей могут быть связаны с описаниями среды безопасности и требуемого уровня доверия к информационной системе, выполняемыми при определении профиля защиты информации.

Ограничение по общей стоимости комплекса средств защиты имеет вид $C \le C_{\text{доп}}$, где $C = \sum_{f=1}^{F} \sum_{m=1}^{M_f} \sum_{n=1}^{N_f} C_{mn}^f x_{mn}^f$ — общая стоимость средств за-

щиты, x_{mn}^f — элементы анализируемой матрицы использования средств защиты $\mathbf{X}^f$ вида (1), C_{mn}^f — стоимость n-го средства при его использовании на m-м рубеже защиты при противодействии f-й цели нарушителя. Поскольку другие ограничения вводятся для отдельных целей нарушителя, допустимая общая стоимость комплекса средств защиты также может быть представлена в виде $C_{\text{доп}} = \sum_{f=1}^{F} C_{\text{доп}}^f$, где $C_{\text{доп}}^f$ — допустимая стоимость средств, используемых для противодействия f-й цели нарушителя.

Ограничение по вероятности противодействия комплекса средств защиты f-й цели нарушителя имеет вид $P^f \ge P_{\text{доп}}^f$, $f = 1, 2, ..., F$, где $P^f = 1 - \sum_{m=1}^{M_f} \prod_{n=1}^{N_f} \left(1 - P_{mn}^f x_{mn}^f\right)$ — вероятность успешного функционирования комплекса средств защиты при противодействии f-й цели нарушителя, x_{mn}^f — элементы анализируемой матрицы использования средств защиты $\mathbf{X}^f$ вида (1). Допустимая величина вероятности противодействия $P_{\text{доп}}^f$ определяется средой безопасности информационной системы.

Ограничение по риску достижения нарушителем своих целей имеет вид $R^f \le R_{\text{доп}}^f$, $f = 1, 2, ..., F$, где R^f — риск при попытке достижения нарушителем f-й цели. Допустимая величина риска $R_{\text{доп}}^f$ определяется требуемым уровнем доверия к информационной системе и при оценке информационной безопасности ИУС характеризует допустимый при попытке достижения нарушителем f-й цели риск потерь информационных активов ИУС — информации, циркулирующей в системе, используемой для управления прикладным процессом и полученной в результате выполнения этого прикладного процесса.

Ограничение по риску достижения нарушителем своих целей является наиболее общим и взаимосвязано с двумя другими ограничениями. Риск потерь информационных активов в общем случае представляет собой произведение вероятности угрозы, вероятности реализации данной угрозы и ущерба, наносимого при реализации данной угрозы [7, 8]. С учетом введенных обозначений риск R^f при попытке достижения нарушителем f-й цели связан с вероятностью успешного функционирования комплекса средств защиты P^f при противодействии f-й цели выражением $R^f = H^f U^f (1 - P^f)$, где H^f — вероятность попытки достижения нарушителем f-й цели; U^f — ущерб, наносимый нарушителем при достижении f-й цели. Величина R^f, как и величина P^f, зависит от элементов x_{mn}^f анализируемой матрицы использования средств защиты $\mathbf{X}^f$ вида (1) и вероятностей P_{mn}^f, а величина ущерба U^f, как правило, является исходной при определении допустимой стоимости средств защиты $C_{\text{доп}}^f$.

При заданных элементах множеств A, B и Z их конечное число позволяет получить решение сформулированной оптимизационной задачи в виде матриц использования средств защиты $\mathbf{X}_{\text{opt}}^f$, $f = 1, 2, ..., F$, удовлетворяющих условию (2), за конечное, пусть большое число шагов. В дальнейшем для полученного решения проверяется выполнение ограничений, и оно принимается или отбрасывается. Для построения алгоритма поиска оптимального решения для конкретных информационной системы и цели нарушителя удобно использование графового метода, основанного на представлении процесса реализации и предотвращения угроз нарушителя в виде направленного графа [5, 9].

Состояния графа реализации угроз соответствуют различной степени достижения цели нарушителя, а переходы между состояниями — последовательности реализации угроз. Полагается, что нарушитель достигает свою цель при реализации одной или нескольких (в предельном случае — всех) угроз, соответствующих данной цели, а в случае предотвращения системой защиты информации на одном из рубежей защиты одной из последовательно реализуемых угроз обеспечивается предотвращение достижения нарушителем соответствующей цели. В зависимости от принятых в информационной системе способа доступа и технологии информационного обмена угрозы и соответствующие им рубежи защиты информации могут быть связаны с преодолением тех или иных структурных элементов системы или уровней эталонной модели информационных систем [3, 10].

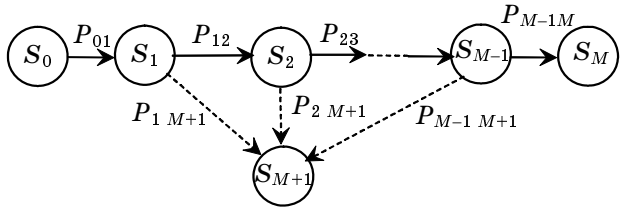
В общем случае при противодействии системы защиты информации f-й цели нарушителя граф реализации угроз включает множество из M_{f+2} состояний $\mathrm{S} = \left\{S_0, S_1, \ldots, S_{M_f}, S_{M_f+1}\right\}$, где S_0 — исходное состояние (отсутствие угроз); S_{M_f} — состояние реализации всех M_f угроз (достижение f-й цели нарушителем); S_m — состояние реализации m из M_f угроз; S_{M_f+1} — состояние предотвращения достижения f-й цели нарушителем. Вероятности состояний — $P(S_m)$, $m = 0, 1, ..., M_f, M_f + 1$. Переходы между состояниями определяются логической (ожидаемой) последовательностью реализации угроз $A_1^f, A_2^f, \ldots, A_{M_f}^f$ и матрицей $\mathbf{X}^f$. Вероятности переходов из m-го в n-е состояние P_{mn} соответствуют вероятностям P_{mn}^f, входящим в выражение (2). Оптимальной матрице $\mathbf{X}_{\text{opt}}^f$ соответствует набор значений x_{mn}^f, дающий максимальную вероятность $P(S_{M_f+1})$ перехода системы в состояние S_{M_f+1}, что соответствует выполнению условия (2).

Вид графа реализации угроз зависит от конкретной информационной системы, ее среды и целей безопасности. Предположим, что для достижения своей цели нарушитель может реализовать от одной до M угроз. На рис. 1 и 2 приведены две

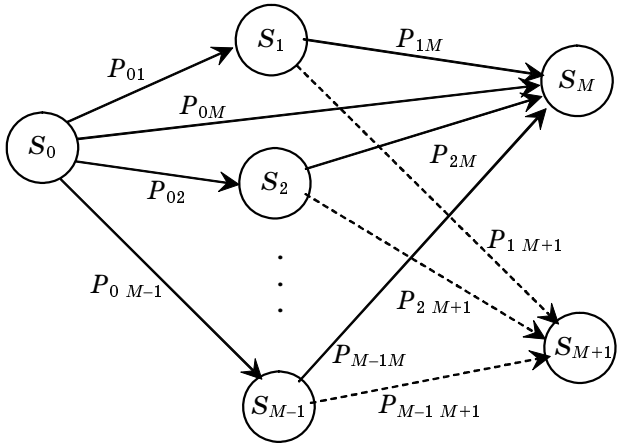
предельные формы графа реализации угроз. На рис. 1 показан граф реализации угроз, в котором цель нарушителя достигается только при реализации всех возможных угроз, что характерно для несанкционированного доступа к проводным сетям. На рис. 2 представлен граф реализации угроз, в котором цель нарушителя может быть достигнута (с различными вероятностями) при реализации любого числа угроз, что характерно для несанкционированного доступа к радиосетям. В обоих случаях полагается, что предотвращение каждой из угроз на соответствующем рубеже защиты позволяет предотвратить достижение цели нарушителя. В первом случае (см. рис. 1) при выполнении $P_{mM+1} = 1$ для одного из значений $m = 1, 2, ..., M-1$ обеспечивается предотвращение достижения цели нарушителя. Во втором случае (см. рис. 2) возможности достижения цели нарушителя при реализации $M_1 < M$ угроз соответствуют вероятности переходов $P_{mM} = 1$ и $P_{mM+1} = 0$ для всех значений $m = M_1, M_1 + 1, ..., M - 1$.

Для распределенных ИУС с каналами беспроводного доступа характерны более сложные графы реализации угроз, чем графы, приведенные на рис. 1 и 2. В них цели нарушителя могут достигаться при реализации различного числа угроз и при различных последовательностях их реализации. Это обусловлено тем, что такие ИУС представляют собой комбинированные сети, включающие проводной и беспроводной сегменты. Среда их безопасности определяется, прежде всего, угрозами, действующими в беспроводном сегменте сети. Нарушитель, не имея физического доступа к сетевому оборудованию и находясь в зоне радиопокрытия, имеет возможность устанавливать логическую связь с точкой радиодоступа в сеть. При этом имеют место широкие возможности несанкционированного доступа нарушителя к радиоканалам передачи данных в пассивном и активном режимах и различные варианты достижения им своих целей. Так, в пассивном режиме нарушитель может осуществлять мониторинг («прослушивание» каналов) с анализом трафика всей сети или с перехватом пакетов, передаваемых по отдельным каналам, а в активном режиме — передавать ложные сообщения или загружать сеть через точку радиодоступа, добиваясь нарушения информационного обмена в сети вследствие отказа в обслуживании. Кроме того, нарушитель может осуществлять эти и другие угрозы одновременно.

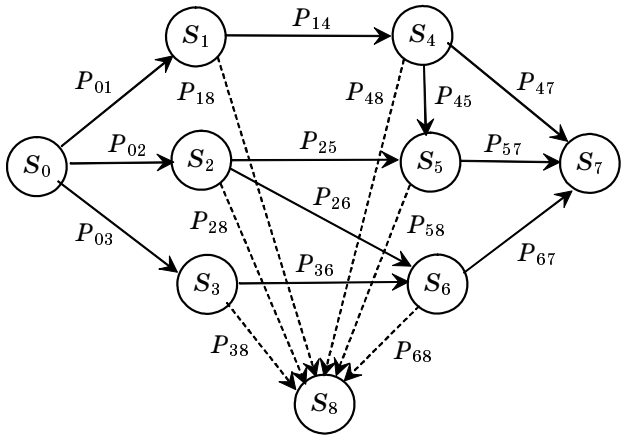
Пример графа реализации угроз сложной структуры, характерной для ИУС с каналами беспроводного доступа, приведен на рис. 3. Граф соответствует информационной системе и некоторой цели нарушителя, для достижения которой он может реализовать $M = 7$ угроз. При этом цель может достигаться при различных последовательностях реализации угроз, определяемых переходами графа состояний. Для решения поставленной задачи графовым методом при подобной произвольной структуре графа он может быть путем ранжирования приведен к виду, показанному на рис. 4. Здесь все состояния распределены по уровням от уровня 0 (начальное состояние S_0) до уровня 4 (заключительные состояния S_7 и S_8) и исключены переходы между состояниями в пределах каждого уровня. Для этого на уровнях 2 и 3 введены фиктивные состояния S'_4, S'_5, S'_6, S'_8, S''_8 и переходы между ними и соответствующими действи-



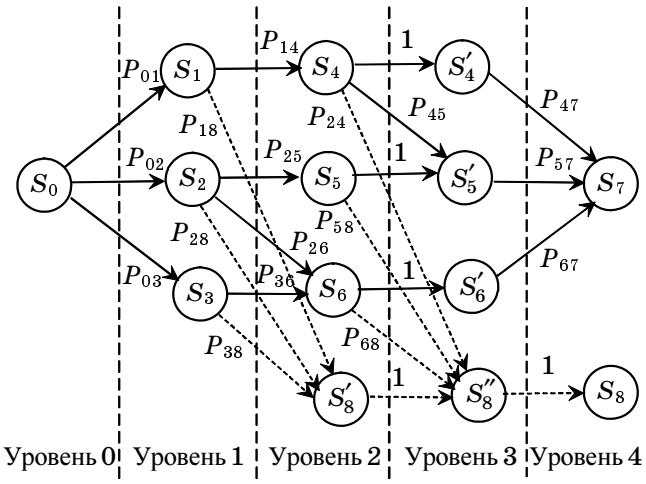
■ ***Рис. 1.*** *Граф реализации угроз, в котором цель нарушителя достигается только при реализации всех возможных угроз*



■ ***Рис. 2.*** *Граф реализации угроз, в котором цель нарушителя может быть достигнута при реализации любого числа угроз*



■ ***Рис. 3.*** *Граф реализации угроз, в котором цель нарушителя может достигаться при различных последовательностях реализации $M = 7$ угроз*



■ ***Рис. 4.*** *Граф реализации угроз, полученный в результате ранжирования графа, приведенного на рис. 3*

тельными состояниями, осуществляемые с вероятностью, равной 1. В результате граф реализации угроз приобретает структуру, удобную для исследования стандартными методами анализа направленных графов.

Рассматриваемая задача оптимизации состава комплекса средств защиты информации распределенной ИУС относится к классу задач дискретной оптимизации. Ее решение графовым методом состоит в определении вероятности нахождения системы в заключительном состоянии S_8 для различных значений вероятностей переходов между состояниями P_{mn}, соответствующими использованию различных средств защиты. При небольшом числе состояний графа решение может быть найдено путем прямого перебора цепей, ведущих от начального состояния S_0 к заключительному состоянию S_8. При большом числе состояний графа для поиска решения может быть использован метод динамического программирования и его модификации, например, рекомендуемый для решения подобных задач метод встречного решения функциональных уравнений [9].

В условиях недостаточной статистической обеспеченности и динамичного изменения условий реализации угроз, характерных для задач защиты информации [9, 11], наиболее сложным может оказаться задание вероятностных характеристик успешного функционирования средств защиты и попыток достижения нарушителем различных целей. В этом случае получают распространение экспертные оценки вероятностных характеристик и методы нечеткого вывода, а для контроля за изменением условий реализации угроз в современных информационных системах в состав комплекса средств защиты включаются средства мониторинга безопасности. Не выполняя непосредственно функций защиты, средства мониторинга позволяют оценить текущее состояние среды безопасности и обеспечить более эффективное функционирование средств защиты за счет уточнения исходных данных, для которых оптимизируется состав комплекса средств защиты.

Литература

1. Инфокоммуникационные сети: архитектура, технологии, стандартизация / Под ред. А. А. Сахнина. М.: Радио и связь, 2004. 208 с.
2. Широкополосные беспроводные сети передачи информации / В. М. Вишневский, А. И. Ляхов, С. Л. Портной, И. В. Шахнович. М.: Техносфера, 2005. 592 с.
3. **Устинов Г. Н.** Основы информационной безопасности систем и сетей передачи данных. М.: СИНТЕГ, 2000. 248 с.
4. Теоретические основы информатики и информационная безопасность / Под ред. В. А. Минаева и В. Н. Саблина. М.: Радио и связь, 2000. 468 с.
5. Обеспечение информационной безопасности в экономической и телекоммуникационной сферах / Под ред. Е. М. Сухарева. М.: Радиотехника, 2003. 216 с.
6. ГОСТ Р ИСО/МЭК 15408–2001. Информационная технология. Методы и средства обеспечения безопасности информационных технологий. Ч. 1–3. М.: Изд-во стандартов, 2002.
7. **Мальцев Г. Н., Моторин Н. М.** Использование риск-анализа при оценке функционирования сложных технических систем передачи информации // Проблемы риска в технической и социальной сферах: Сб. науч. тр. Вып. 4. Риск информационной опасности. СПб.: СПбГТУ, 2005. С. 59–62.
8. **Мальцев Г. Н., Теличко В. В.** Метод определения риска потерь активов при разработке профиля защиты информации транспортной сети передачи данных // Информационные технологии на железнодорожном транспорте: Докл. XII Междунар. конф. «Инфотранс-2007». СПб.: ПГУПС, 2007. С. 65–70.
9. Модели развития технических разведок и угроз безопасности информации / Под ред. Е. М. Сухарева. М.: Радиотехника, 2003. 142 с.
10. **Зима В. М., Молдовян А. А., Молдовян Н. А.** Безопасность глобальных сетевых технологий. СПб.: Изд-во СПбГУ, 1999. 368 с.
11. **Гаценко О. Ю.** Защита информации. Основы организационного управления. СПб.: Сентябрь, 2001. 228 с.