УДК 004.056 Дата подачи статьи: 03.04.17
DOI: 10.15827/0236-235X.120.690-698 2017. Т. 30. № 4. С. 690–698

МЕТОДИЧЕСКИЙ ПОДХОД К ФОРМИРОВАНИЮ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К СИСТЕМЕ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ И ЕГО ПРОГРАММНАЯ РЕАЛИЗАЦИЯ

Е.Б. Дроботун, к.т.н., докторант, drobotun@xakep.ru
(Военная академия воздушно-космической обороны им. Маршала Советского Союза Г.К. Жукова, ул. Жигарева, 50, г. Тверь, 170022, Россия)

Одной из основных стадий разработки и построения автоматизированных систем управления различного назначения в защищенном исполнении является формирование функциональных требований к разрабатываемой автоматизированной системе, в том числе и функциональных требований к защите автоматизированной системы от компьютерных атак и других видов информационно-технического воздействия.

Оптимально сформированные и обоснованные функциональные требования к системе защиты от компьютерных атак позволят, с одной стороны, обеспечить необходимый уровень защиты автоматизированной системы, а с другой – минимизировать потребление вычислительных и человеческих ресурсов защищаемой автоматизированной системы, объем которых в любой автоматизированной системе ограничен и конечен.

Одним из возможных путей формирования и обоснования оптимальных функциональных требований к системе защиты от компьютерных атак является применение риск-ориентированного подхода к формированию и обоснованию этих требований, который заключается в выявлении степени опасности и вероятности проявления возможных угроз безопасности в отношении защищаемой автоматизированной системы.

В статье предлагается методический подход к формированию функциональных требований к системам защиты от компьютерных атак для автоматизированных систем управления, основанный на оценке риска угроз безопасности информации в автоматизированной системе и угроз ее безопасного функционирования.

Применение предложенного методического подхода позволит сформировать оптимальные функциональные требования к системе защиты от компьютерных атак для автоматизированных систем управления различного назначения, реализация которых дает возможность достичь оптимального распределения ресурсов автоматизированной системы для обеспечения функционирования системы защиты от компьютерных атак.

Ключевые слова: *автоматизированная система, угроза безопасности автоматизированной системы, компьютерная атака, функциональные требования, анализ риска.*

Основой для разработки и построения системы защиты от компьютерных атак для АСУ являются функциональные требования, которые формируются в соответствии с подходом к построению автоматизированных систем в защищенном исполнении [1, 2].

Оптимально сформированные и обоснованные функциональные требования к системе защиты от компьютерных атак позволят спроектировать и построить рациональную систему защиты от компьютерных атак, которая, с одной стороны, обеспечит необходимый уровень защиты, а с другой, будет потреблять минимальное количество вычислительных и человеческих ресурсов защищаемой системы, что, в свою очередь, позволит минимизировать снижение эффективности защищаемой системы вследствие введения в ее состав системы защиты от компьютерных атак.

В настоящее время процесс формирования требований к системам защиты информации для автоматизированных систем различного назначения регламентируется рядом нормативно-методических документов, описание и порядок применения которых приведены в [3, 4].

Анализ данных источников показывает, что их применение не в полной мере позволяет сформировать оптимальные требования к системе защиты от компьютерных атак для АСУ различного назначения в силу ряда причин:

– их ориентация в большей степени на защиту хранящейся и (или) обрабатываемой в АСУ информации от несанкционированного доступа с целью предотвращения ее утечек (в то время как компьютерные атаки могут осуществляться не только для получения несанкционированного доступа к информации и ее хищения, но и чтобы нарушить правильность функционирования АСУ);

– гарантированный подход к защите информации (то есть достижение максимально возможной степени защищенности без учета критичности защищаемых ресурсов);

– несовершенство существующих методик построения моделей угроз безопасности для современных АСУ (ориентация существующих методик в большей степени на угрозы несанкционированного доступа к информации и ведения внешней технической компьютерной разведки).

Одним из возможных путей формирования и обоснования оптимальных функциональных требований к системе защиты от компьютерных атак является применение методического подхода, основанного на анализе и оценке рисков угроз безопасности информации в автоматизированной системе и ее безопасного функционирования.

Данный методический подход базируется на следующих основных принципах:

– прогнозирование угроз безопасности в защищаемой АСУ;

– достаточность мер защиты от компьютерных атак для некритичных компонентов и информационных ресурсов АСУ;

– максимальная защита критичных информационных ресурсов АСУ от компьютерных атак.

Для формального описания предлагаемого методического подхода к формированию функциональных требований к системам защиты от компьютерных атак необходимо определить несколько положений.

Введем следующие обозначения: T – множество угроз безопасности АСУ; K – множество видов и способов реализации компьютерных атак; Q – множество элементов, входящих в состав АСУ, при этом $Q = A \cup S \cup C \cup H$, где A – множество программно-аппаратных компонентов АСУ; S – множество компонентов ПО АСУ; C – множество информационных ресурсов, хранящихся и (или) обрабатываемых в АСУ; H – множество лиц, эксплуатирующих и обслуживающих АСУ.

Положение 1. Имеется эффективный метод построения соответствия Φ_1 из множества T в множество Q, который определяется по следующему правилу: $(\forall\, t \in T)\ (\forall\, q \in Q)(t\Phi_1 q \Leftrightarrow$ угроза t представляет опасность для элемента q).

Пусть $T^* = \{t_i^* \mid i = 1, 2, \ldots, I\}$ – область определения соответствия Φ_1, то есть $T^* = Dom\Phi_1 \subseteq T$. Ограничение соответствия Φ_1 на подмножество T^* обозначим через Φ^*_1.

Соответствие Φ^*_1 может быть представлено посредством графа $G(\Phi^*_1)$ (рис. 1).

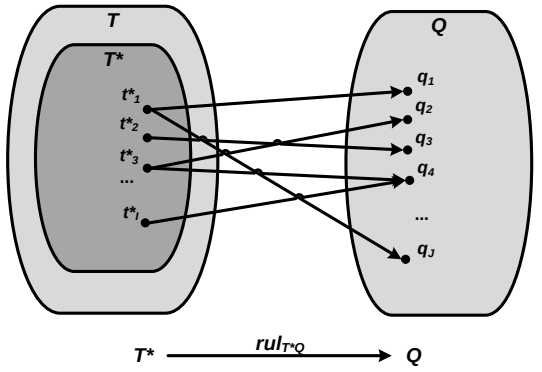

Рис. 1. Пример сопоставления элементов множества T элементам множества Q*

Fig. 1. The example of comparing the elements of the set T to the elements of the set Q*

Это соответствие может быть также представлено в виде булевой матрицы rul_{T*Q} размерности $I \times J$:

$$rul_{T*Q} = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1J} \\ \gamma_{21} & \gamma_{22} & \cdots & \gamma_{2J} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{I1} & \gamma_{I2} & \cdots & \gamma_{IJ} \end{pmatrix},$$

где $\gamma_{ij} = \begin{cases} 1, \text{ если угроза } t_i^* \text{ представляет} \\ \quad \text{опасность для элемента } q_j, \\ 0 \text{ в противном случае,} \end{cases}$

$i = \overline{1, I}$; $j = \overline{1, J}$.

Положение 2. Имеется эффективный метод построения соответствия Φ_2 из множества K в множество T, которое определяется по следующему правилу: $(\forall k \in K)\ (\forall t \in T)(k\Phi_2 t \Leftrightarrow$ угроза t может быть реализована посредством компьютерной атаки k).

Пусть $K^* = \{k_l^* \mid l = 1, 2, \ldots, L\}$ – область определения соответствия Φ_2. Тогда в соответствии с положением 1 будем иметь $Im\Phi_2 = T^*$. Ограничение соответствия Φ_2 на подмножество K^* обозначим через Φ^*_2.

На рисунке 2 показана геометрическая реализация соответствия Φ^*_2 посредством графа $G(\Phi^*_2)$.

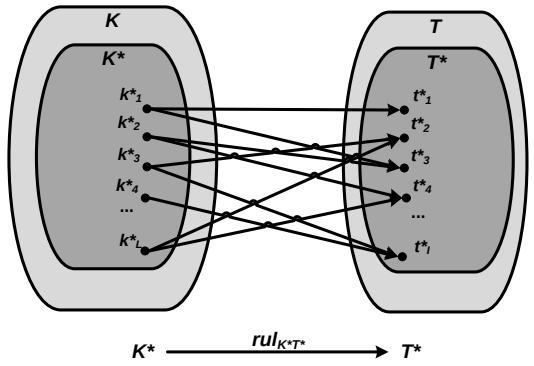

Рис. 2. Пример сопоставления элементов множества K элементам множества T**

Fig. 2. The example of comparing the elements of the set K to the elements of the set T**

Это соответствие можно представить посредством матрицы rul_{K*T*} размерности $L \times I$:

$$rul_{K*T*} = \begin{pmatrix} \tau_{11} & \tau_{12} & \cdots & \tau_{1I} \\ \tau_{21} & \tau_{22} & \cdots & \tau_{2I} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{L1} & \tau_{L2} & \cdots & \tau_{LI} \end{pmatrix},$$

где $\tau_{il} = \begin{cases} 1, \text{ если угроза } t_i^* \text{ может быть реализована} \\ \quad \text{посредством компьютерной атаки } k_l^*, \\ 0 \text{ в противном случае,} \end{cases}$

$l = \overline{1, L}$; $i = \overline{1, I}$.

Положение 3. Имеется эффективный метод построения соответствия Φ_3 из множества K в множество Q, которое определяется по следующему правилу: $(\forall k \in K)\ (\forall q \in Q)(k\Phi_3 q \Leftrightarrow$ элемент q есть потенциальный объект компьютерной атаки k).

Наличие эффективного метода этого положения является следствием существования соответствующих методов положений 1 и 2.

В частности, $Dom\Phi_3 = K^* \subseteq K$. Ограничение соответствия Φ_3 на подмножество K^* множества K обозначим через Φ^*_3. Графовая реализация Φ^*_3 показана на рисунке 3.

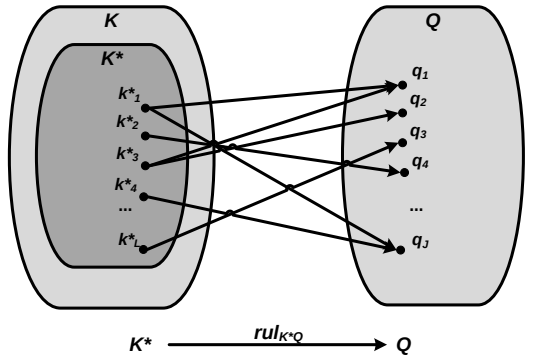

Рис. 3. Пример сопоставления элементов множества K элементам множества Q*

Fig. 3. The example of comparing the elements of the set K to the elements of the set Q*

Это соответствие можно представить посредством матрицы rul_{K*Q} размерности $L \times J$:

$$rul_{K*Q} = \begin{pmatrix} \mu_{11} & \mu_{12} & \cdots & \mu_{1J} \\ \mu_{21} & \mu_{22} & \cdots & \mu_{2J} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{L1} & \mu_{L2} & \cdots & \mu_{LJ} \end{pmatrix},$$

где $\mu_{jl} = \begin{cases} 1, \text{ если элемент } q_j \text{ – потенциальный} \\ \quad \text{объект компьютерной атаки } k^*_l, \\ 0 \text{ в противном случае,} \end{cases}$

$j = \overline{1, J}$; $l = \overline{1, L}$.

Матрицы rul_{K*T*} и rul_{T*Q} как формальные воплощения эффективности методов положений 2 и 1 соответственно определяют матрицу rul_{K*Q} как формальный аналог эффективности метода положения 3 путем логического произведения матриц rul_{K*T*} и rul_{T*Q}: $rul_{K*Q} = rul_{K*T*} \times rul_{T*Q}$.

Перейдем к описанию технологий выявления количественных характеристик рисков нарушения безопасности АСУ при проведении на нее компьютерных атак.

С этой целью каждому элементу q_j множества Q ставится в соответствие весовой коэффициент w_j, характеризующий важность (с позиций безопасности АСУ – критичность) этого элемента $(j = \overline{1, J})$. В общем случае не исключается возможность того, что один и тот же весовой коэффициент может быть поставлен в соответствие различным элементам множества Q (рис. 4).

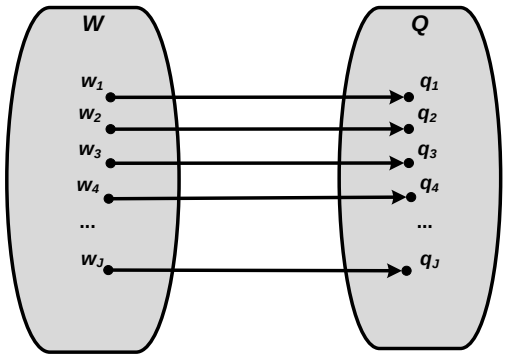

Рис. 4. Пример отображения множества W на множество Q

Fig. 4. The example of mapping of the set W on the set Q

Возможность компьютерной атаки на какой-либо объект (компонент) АСУ характеризуется вероятностью этой атаки в отношении атакуемого объекта (компонента) АСУ. Данная вероятность определяется возможностями (потенциалом и мотивацией) нарушителя (субъекта, осуществляющего атаку), наличием или отсутствием уязвимостей в атакуемом объекте и степенью их опасности, а также наличием угрозы, которая может быть реализована данной компьютерной атакой в отношении атакуемого объекта [5–7]:

$$p = f\,(Pt_{\text{НАР}}, M_{\text{НАР}}, V_{\text{УЯЗВ}}, B_{\text{УГР}}), \qquad (1)$$

где $Pt_{\text{НАР}}$ – потенциал нарушителя, зависящий от уровня его общей технической осведомленности, осведомленности об особенностях построения и функционирования атакуемой АСУ и его технического оснащения (наличия или отсутствия технических средств, необходимых для проведения атаки) [5]; $M_{\text{НАР}}$ – мотивация нарушителя; $V_{\text{УЯЗВ}}$ – уровень опасности уязвимостей, имеющихся в атакуемом объекте (как правило, определяется с помощью широко известной и применяемой методики CVSS [8, 9]); $B_{\text{УГР}}$ – булева функция, определяющая наличие или отсутствие угрозы безопасности при проведении компьютерной атаки на атакуемый объект:

$$B_{\text{УГР}} = \begin{cases} 1, \text{ если компьютерная атака несет угрозу} \\ \quad \text{атакуемому объекту,} \\ 0 \text{ в противном случае.} \end{cases}$$

$B_{\text{УГР}}$ может быть определено из матрицы rul_{K*Q}, которая показывает наличие или отсутствие угрозы при проведении l-й компьютерной атаки на j-й элемент АСУ. При этом от булевой матрицы rul_{K*Q} можно перейти к матрице вероятностей проведения компьютерных атак в отношении АСУ в целом:

$$P_{K*Q} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1J} \\ p_{12} & p_{22} & \cdots & p_{2J} \\ \vdots & \vdots & \ddots & \vdots \\ p_{L1} & p_{L2} & \cdots & p_{LJ} \end{pmatrix},$$

где L – число видов и способов компьютерных атак (из множества K^*); J – число компонентов, входящих в состав АСУ, а элементы (p_{lj}, $l = \overline{1, L}$; $j = \overline{1, J}$) этой матрицы определяются в соответствии с выражением (1) по методике, изложенной в [7].

Используя полученную матрицу вероятностей проведения компьютерных атак на АСУ и (весовые) коэффициенты важности (критичности) составных компонентов АСУ из множества W, можно определить матрицу рисков нарушения безопасности АСУ при проведении компьютерных атак:

$$R = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1J} \\ r_{12} & r_{22} & \cdots & r_{2J} \\ \vdots & \vdots & \ddots & \vdots \\ r_{L1} & r_{L2} & \cdots & r_{LJ} \end{pmatrix}, \qquad (2)$$

где, как и ранее, L – число видов и способов компьютерных атак; J – число компонентов, входящих в состав АСУ, а элементы этой матрицы r_{lj} определяются следующим образом: $r_{lj} = p_{lj} \times w_j$ при $i = \overline{1, L}$; $j = \overline{1, J}$; w_j – коэффициент, характеризующий важность (критичность) j-го компонента из состава АСУ.

Таким образом, элемент матрицы рисков r_{lj} характеризует риск нарушения безопасности j-го компонента АСУ вследствие проведения на него l-й компьютерной атаки. Под риском нарушения безопасности посредством компьютерной атаки в данном случае понимается сочетание вероятности реализации той или иной угрозы в отношении того или иного компонента АСУ с помощью той или иной компьютерной атаки и степени тяжести последствий реализации этой угрозы для атакуемой АСУ [10–12].

Полученная ранее матрица рисков нарушения безопасности АСУ (2) является основой для формирования функциональных требований к системе защиты от компьютерных атак.

Для описания этих требований сформулируем в дополнение к положениям 1–3 еще ряд положений.

Положение 4. Предположим, что для каждой компьютерной атаки из множества K^* можно эффективным способом определить совокупность средств защиты, способных полностью нейтрализовать данную компьютерную атаку. То есть каждому элементу множества K^* можно поставить в соответствие определенную совокупность средств защиты S^*_i ($i = \overline{1, L}$, где L, как и ранее, – число видов и способов компьютерных атак), являющуюся подмножеством общего множества S, элементы которого представляют собой отдельные составляющие системы защиты от компьютерных атак в целом (рис. 5). На рисунке 5 для наибольшей наглядности различные подмножества $S^*_{l_1}$ и $S^*_{l_2}$, $1 \le l_1 < l_2 \le L$, изображены как непересекающиеся, хотя в общем случае их пересечения и даже совпадения не исключаются.

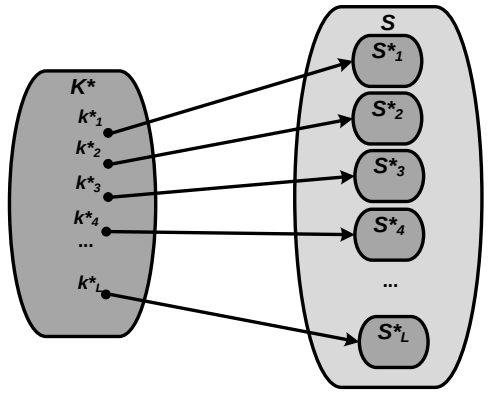

Рис. 5. Пример сопоставления каждой компьютерной атаке совокупности средств защиты

Fig. 5. The example of comparing each computer attack to the set of protection means

Обозначим через S^* множество $\bigcup_{l=1}^{L} S_l$. Будем полагать, что $S^* = \{s^*_1, s^*_2, ..., s^*_R\}$. В общем случае S^* может не совпадать с S, то есть $S^* \subseteq S$.

Каждое множество S_i, которое входит в виде подмножества во множество S, включает в себя определенное число средств защиты (число элементов множеств S_1, S_2, …, S_i зависит от видов и способов компьютерных атак, для нейтрализации которых они предназначены). Распределение средств защиты по соответствующим совокупностям задается матрицей защиты:

$$H = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1R} \\ h_{21} & h_{22} & \cdots & h_{2R} \\ \vdots & \vdots & \ddots & \vdots \\ h_{L1} & h_{L2} & \cdots & h_{LR} \end{pmatrix}, \qquad (3)$$

где L – число видов и способов компьютерных атак; R – число средств защиты множества S^*; элементы этой матрицы h_{lr} определяются следующим образом:

$$h_{lr} = \begin{cases} 1, \text{ если средство } s^*_r \text{ защиты необходимо} \\ \quad \text{для нейтрализации компьютерной атаки } k^*_l, \\ 0 \text{ в противном случае.} \end{cases}$$

Пример 1. Для $I = 5$ (число видов и способов компьютерных атак) и $J = 6$ (число средств защиты) зададим распределение средств защиты (табл. 1).

Таблица 1

Пример распределения средств защиты

Table 1

The example of protection means distribution

Вид и способ компьютерной атаки	Средство защиты					
	s^*_1	s^*_2	s^*_3	s^*_4	s^*_5	s^*_6
k_1	1	1	0	1	0	0
k_2	1	0	1	0	1	0
k_3	0	1	0	0	0	1
k_4	1	0	0	0	0	1
k_5	0	1	1	1	0	1

То есть применительно к этому примеру будем иметь: $S^* = \{s_1^*, s_2^*, s_3^*, s_4^*, s_5^*, s_6^*\}$. $S_1^* = \{s_1^*, s_2^*, s_4^*\}$; $S_2^* = \{s_1^*, s_3^*, s_5^*\}$; $S_3^* = \{s_2^*, s_6^*\}$; $S_4^* = \{s_1^*, s_6^*\}$; $S_5^* = \{s_2^*, s_3^*, s_4^*, s_6^*\}$.

Положение 5. Будем полагать, что каждое средство защиты s_r^* ($r = \overline{1, R}$) имеет определенный набор свойств X_r, характеризующих степень обеспечения ими защиты: $X_r = \{x_{r1}, x_{r2}, \ldots, x_{rN}\}$, где N – количество свойств этого средства защиты. При этом все множество свойств X_r можно разделить на k подмножеств таким образом, что $X_r = \{X_{r1} \cup X_{r2} \cup \ldots \cup X_{rk}\}$, при этом $X_{r1} \subset X_{r2}$, $X_{r2} \subset X_{r3}$, …, $X_{rk-1} \subset X_{rk} = X_r$ (рис. 6).

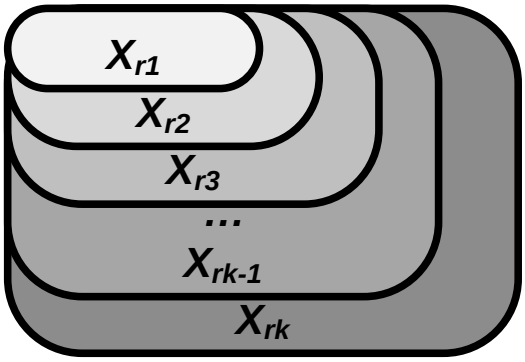

Рис. 6. Деление множества X_r на подмножества

Fig. 6. The division of the set X_r into subsets

Через s_{rt}^* обозначим средство защиты s_r^*, совокупность свойств которого X_r ограничена до подсовокупности X_{rt}, $t = 1, 2, \ldots, k$.

Тогда средство защиты s_{r1}^* как имеющее набор свойств X_{r1} будет обеспечивать минимальную эффективность защиты, потребляя при этом минимальное количество ресурсов для своего функционирования; средство защиты s_{rk}^* как имеющее набор свойств X_{rk} будет обеспечивать максимальную эффективность защиты, потребляя при этом максимальное количество ресурсов для своего функционирования, а средства защиты s_{r2}^*, s_{r3}^*, …, $s_{r\kappa-1}^*$ со свойствами X_{r2}, X_{r3}, …, X_{rk-1} будут обеспечивать промежуточные (между минимальным и максимальным) уровни защиты.

Полагая, что эффективность средств защиты имеет количественную характеризацию, и обозначив через g_t количественную меру эффективности средства защиты s_{rt}^*, а через z_t потребляемые этим средством ресурсы, будем иметь $g_1 < g_2 < \ldots < g_k$ и $z_1 < z_2 < \ldots < z_k$.

Положение 6. Допустим, что каждому элементу x_r множества $X_r = \{x_{ri} \mid i = \overline{1, N}\}$ свойств каждого средства защиты можно поставить в соответствие один из элементов f множества функциональных требований F. Будем полагать при этом, что требование f_i задает условие наделения этого средства защиты свойством x_{ri}, $i = \overline{1, N}$ (рис. 7).

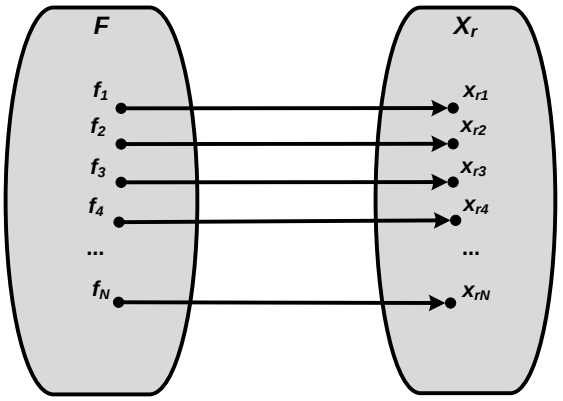

Рис. 7. Пример сопоставления элементов множества функциональных требований элементам множества свойств средства защиты

Fig. 7. The example of comparing elements of the functional requirements set to elements of the protection means set

Положение 7. Для каждого оценочного значения r_{lj} риска из матрицы риска (7) можно определить свое подмножество свойств $X_{rl_t} \in \{X_{r1}, X_{r2}, \ldots, X_{rk}\}$, $t = \overline{1; k}$, из множества X_r следующим образом: минимальному значению риска соответствует множество свойств X_{r1}, максимальному значению риска соответствует множество свойств X_{rk}, промежуточным значениям риска соответствуют промежуточные множества свойств X_{r2}, X_{r3}, …, X_{rk-1} по возрастанию. При этом k будет являться уровнем реализации свойств каждого отдельного средства.

Принцип формирования функциональных требований к системе защиты АСУ от компьютерных атак заключается в выборе необходимого набора свойств X_r (и соответствующих этим свойствам функциональных требований F) для каждого средства защиты s, входящего в совокупности средств защиты S^*_1, S^*_2, …, S^*_R, из которых, в свою очередь, строится система защиты S от компьютерных атак.

Правило выбора необходимого набора свойств основано на положении 7. Для начала определяется количество уровней риска (наиболее приемлемыми являются четыре уровня риска: отсутствует, низкий, средний, высокий [7]), а затем граничные значения риска для каждого уровня.

После этого формируют множества свойств X_{r1}, X_{r2}, …, X_{rk} для каждого средства (где k – число уровней значений риска) на основании положения 7. Далее, используя матрицу распределения средств защиты (3), для каждой компьютерной атаки из множества K^* определяют необходимые совокупности средств защиты, а используя мат-

рицу риска (2), необходимые наборы свойств для каждой совокупности средств защиты, формируя при этом матрицу M уровней реализации свойств средств защиты:

$$M = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1R} \\ m_{21} & m_{22} & \cdots & m_{2R} \\ \vdots & \vdots & \ddots & \vdots \\ m_{L1} & m_{L2} & \cdots & m_{LR} \end{pmatrix},$$

где L – число видов и способов компьютерных атак; R – число средств защиты, а элементы этой матрицы m_{ij}, $i = \overline{1, L}$, $j = \overline{1, R}$, определяются числовым значением уровня реализации свойств для каждого средства.

Пример 2. Исходя из матрицы распределения средств защиты (табл. 1) и следующих уровней риска для компьютерных атак (по методике, изложенной в [7]): k_1 – высокий, k_2 – низкий, k_3 – отсутствует, k_4 – средний, k_5 – высокий, определим матрицу уровней реализации свойств средств защиты (табл. 2).

Таблица 2

Пример матрицы уровней реализации свойств средств защиты

Table 2

The example of the matrix of implementation levels of protection means properties

Вид, способ компьютерной атаки и уровень ее риска	Средство защиты					
	s^*_1	s^*_2	s^*_3	s^*_4	s^*_5	s^*_6
k_1 – высокий	4	4	0	4	0	0
k_2 – низкий	2	0	2	0	2	0
k_3 – отсутствует	0	1	0	0	0	1
k_4 – средний	3	0	0	0	0	3
k_5 – средний	0	3	3	3	0	3

При этом использовалось соответствие уровней риска компьютерных атак уровням реализации свойств средств защиты (табл. 3).

Таблица 3

Соответствие уровней риска компьютерных атак уровням реализации свойств средств защиты

Table 3

Correspondence of computer attacks risk levels with implementation levels of protection means properties

Уровень риска	Уровень реализации свойств средств защиты
Высокий	4
Средний	3
Низкий	2
Отсутствует	1

Таким образом, совокупность S^* будет представлять собой объединение следующих средств защиты: $S^* = \{\{s_1^*(4), s_2^*(4), s_4^*(4)\}, \{s_1^*(2), s_3^*(2), s_5^*(2)\}, \{s_2^*(1), s_6^*(1)\}, \{s_1^*(3), s_6^*(3)\}, \{s_2^*(3), s_3^*(3), s_4^*(3), s_6^*(3)\}\}$, где $s_i^*(k)$ следует понимать как i-е средство с k-м уровнем реализации свойств.

Следует отметить, что сформированное таким образом множество S^* (которое по сути представляет собой вариант построения системы защиты) обладает избыточностью, от которой можно избавиться, применив следующие правила.

Правило сокращения – если множество S^* содержит несколько одинаковых средств защиты с одинаковым уровнем реализации свойств, то количество этих средств сокращается до одного.

Правило поглощения – если множество S^* содержит несколько одинаковых средств защиты с разными уровнями реализации свойств, то все средства с уровнем реализации свойств, меньшим максимального, поглощаются средством с максимальным уровнем реализации (то есть в множестве S^* остается только функция с максимальным уровнем реализации).

Данные правила реализуются следующим образом:

– в каждом столбце матрицы реализации свойств производится поиск максимального элемента;

– номер столбца будет номером средства защиты, которое включается в систему защиты (если все элементы текущего столбца равны нулю, то средство текущего номера в состав системы защиты не включается);

– уровнем реализации свойств для средства защиты будет максимальное значение текущего столбца матрицы.

Формально это можно записать следующим образом: $S^* \xrightarrow{Сокр,\ Погл} \hat{S}$,

$$\hat{S} = \{s_1^*(\max(m_{11}, m_{21}, ..., m_{L1})), s_2^*(\max(m_{12}, m_{22}, ..., m_{L2})), ..., s_j^*(\max(l_{1R}, l_{2R}, ..., l_{LR}))\}, \quad (4)$$

где m_{ij} – элемент матрицы уровней реализации свойств M.

Пример 3. Исходя из матрицы уровней реализации свойств из примера 2 (табл. 2) и используя выражение (4) сформируем множество $\hat{S}$ следующим образом (рис. 8):

$$\hat{S} = \{s_1^*(4), s_2^*(4), s_3^*(3), s_4^*(4), s_5^*(2), s_6^*(3)\}.$$

После формирования рационального множества средств защиты $\hat{S}$, используя положение 6, можно перейти от множества свойств для каждого средства защиты к множеству функциональных требований, необходимых для реализации этих свойств.

Таким образом, формирование рациональных требований к системе защиты от компьютерных атак будет заключаться в следующем:

– выбор необходимых совокупностей средств защиты $\{S^*_1, S^*_2, \ldots, S^*_L\}$ для каждой компьютерной атаки;

Вид, способ компьютерной атаки и уровень ее риска	Средство защиты					
	s^*_1	s^*_2	s^*_3	s^*_4	s^*_5	s^*_6
k_1 – высокий	4	4	0	4	0	0
k_2 – низкий	2	0	2	0	2	0
k_3 – отсутствует	0	1	0	0	0	1
k_4 – средний	3	0	0	0	0	3
k_5 – средний	0	3	3	3	0	3

Рис. 8. Пример сопоставления множеств свойств X_k значениям риска

Fig. 8. The example of comparing the properties sets X_k to the level of risk

– выбор нужного набора свойств для каждого средства, входящего в совокупности средств защиты;

– приведение полученного множества средств защиты S^* к рациональной форме $\hat{S}$ с использованием правила сокращения и правила поглощения;

– формирование функциональных требований по обеспечению нужного набора свойств для каждого средства защиты, входящего в совокупности средств защиты.

Программный комплекс, позволяющий реализовать предложенный методический подход (рис. 9), должен включать в себя:

– БД угроз информационной безопасности и уязвимостей компонентов информационно-вычислительных (автоматизированных) систем;

– средства оценки степени опасности уязвимостей компонентов информационно-вычислительных систем, потенциала нарушителя информационной безопасности в автоматизированных системах и риска реализации в них угроз безопасности;

– БД профилей функциональных требований к системам защиты от компьютерных атак для различных степеней риска;

– средство формирования функциональных требований (имеющее в составе блоки формирования необходимых совокупностей средств защиты, полного (избыточного) перечня функциональных требований и рационального перечня функциональных требований).

На данный момент в полном объеме реализованы следующие компоненты предполагаемого программного комплекса:

– БД угроз информационной безопасности и уязвимостей компонентов информационно-вычислительных систем (см. http://www.swsys.ru/uploaded/image/2017_4/2017-4-dop/2.jpg);

– программа оценки степени опасности уязвимостей компонентов информационно-вычислительных систем (см. http://www.swsys.ru/uploaded/image/2017_4/2017-4-dop/3.jpg);

– программа оценки потенциала нарушителя безопасности информации (см. http://www.swsys.ru/uploaded/image/2017_4/2017-4-dop/4.jpg).

БД угроз информационной безопасности и уязвимостей компонентов информационно-вычислительных систем разработана на основе информации из банка данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru).

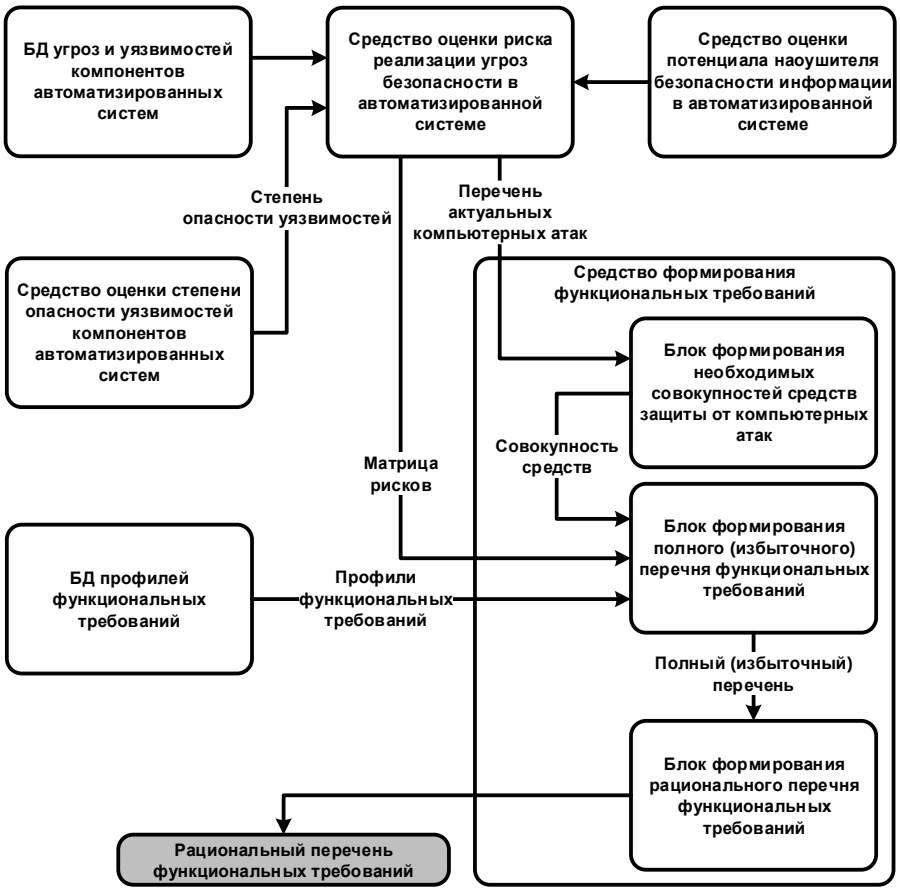

Рис. 9. Общая схема программного комплекса формирования функциональных требований к системе защиты от компьютерных атак

Fig. 9. A general scheme of a software complex forming functional requirements for the computer attack protection system

Информация об угрозах безопасности:

– наименование угрозы;

– идентификатор угрозы (в виде ее порядкового номера);

– описание источника угрозы (вид нарушителя (внутренний или внешний) и его потенциал (отсутствует, низкий, средний или высокий));

– описание объекта воздействия;

– описание последствий реализации угрозы (нарушение целостности, конфиденциальности или доступности информации).

Поиск записей в базе угроз возможен по диапазону идентификаторов, по источнику угрозы, по последствиям реализации угрозы, а также с помощью фильтра поиска на основе произвольных SQL-запросов.

Информация об уязвимостях компонентах информационно-вычислительных систем:

– идентификатор уязвимости;

– наименование уязвимости;

– идентификатор уязвимости, присвоенный ФСТЭК России;

– дата выявления уязвимости;

– идентификаторы других систем описания уязвимостей (CVE, OSVDB и др.);

– наименование ПО, содержащего уязвимость;

– версия ПО;

– наименование операционной системы, для которой характерна данная уязвимость;

– класс уязвимости (уязвимость кода или уязвимость архитектуры);

– базовый вектор оценки CVSS;

– уровень опасности уязвимости по CVSS;

– ссылка на источник информации об уязвимости в Интернете.

Поиск записей в базе возможен по диапазону идентификаторов, по идентификатору ФСТЭК России, по классу уязвимости, по уровню опасности, а также с помощью фильтра поиска по произвольным SQL-запросам.

БД зарегистрирована в государственном реестре БД (рег. №2016620378 от 24.03.2016) (https://github.com/drobotun/Threat_DB).

Программа оценки степени опасности уязвимостей компонентов информационно-вычислительных систем «Калькулятор CVSS» (см. http://www.swsys.ru/uploaded/image/2017_4/2017-4-dop/3.jpg) реализует оценку степени опасности уязвимостей по широко известной и применяемой методике CVSS [8].

Программа разработана в среде Delphi, исходный код доступен по адресу: https://github.com/drobotun/CVSS_Calc.

Программа оценки потенциала нарушителя безопасности информации реализует методику оценки, описанную в [7].

Программа разработана в среде программирования Delphi, исходный код программы доступен по адресу: https://github.com/drobotun/Violator_Calc. Программа зарегистрирована в государственном реестре программ для ЭВМ (рег. № 2016615110 от 16.05.2016).

Средство оценки риска предполагается реализовать в виде программы, работа которой будет основана на приведенных выше положениях и методике, изложенной в [7].

В БД профилей функциональных требований планируется включить профили функциональных требований для средств обнаружения компьютерных атак, средств противодействия компьютерным атакам и для средств устранения последствий применения компьютерных атак для четырех уровней риска реализации угроз (в соответствии с табл. 3).

Средство формирования функциональных требований предполагается реализовать в виде отдельной программы, работа которой будет основана на приведенных выше положениях и правилах сокращения и поглощения.

Применение предложенного методического подхода обеспечивает возможность формирования рациональных функциональных требований, позволяющих спроектировать и построить рациональную систему защиты, которая, с одной стороны, обеспечит необходимый уровень защиты, а с другой – будет потреблять минимальное количество вычислительных и человеческих ресурсов защищаемой АСУ, что, в свою очередь, позволит минимизировать фактор снижения эффективности защищаемой системы вследствие введения в ее состав системы защиты от компьютерных атак.

Литература

1. Основы проектирования и эксплуатации автоматизированных систем управления военного назначения: учеб. пособие; [под ред. В.Л. Лясковского]. М.: Изд-во МГТУ им. Н.Э. Баумана, 2016. 188 с.

2. Малюк А.А., Пазизин С.В., Пригожин Н.С. Введение в защиту информации в автоматизированных системах. М.: Горячая линия–Телеком, 2001. 148 с.

3. Галатенко В.А. Стандарты информационной безопасности: курс лекций; [под ред. В.Б. Бетелина]. М.: ИНТУИТ.РУ, 2006. 264 с.

4. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации; [под ред. А.С. Маркова]. М.: Радио и связь, 2012. 192 с.

5. Гришина Н.В. Модель потенциального нарушителя объекта информатизации // Изв. ЮФУ: Технич. науки. 2003. № 4. Т. 33. С. 356–358.

6. Жуков В.Г., Жукова М.Н., Стефаров А.П. Модель нарушителя прав доступа в автоматизированной системе // Программные продукты и системы. 2012. № 2. С. 75–78.

7. Дроботун Е.Б., Цветков О.В. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя // Программные продукты и системы. 2016. № 3. С. 42–50.

8. Common Vulnerability Scoring System. URL: http://www.first.org/cvss (дата обращения: 12.03.2017).

9. Нурдинов Р.А. Определение вероятности нарушения критических свойств информационного актива на основе CVSS

метрик уязвимостей // Современные проблемы науки и образования. 2014. № 3. URL: http://www.science-edukation.ru/pdf/2014/3/344.pdf (дата обращения: 12.03.2017).

10. Белов В., Голяков А. Терминологическая база теории безопасности // Стандарты и качество. 2004. № 9. С. 48–51.

11. Быков А.А., Порфирьев Б.Н. О взаимосвязи риска с родственными понятиями и терминологии риск-менеджмента // Проблемы анализа риска. 2013. Т. 10. № 4. С. 4–10.

12. Алпеев А.С. Основные понятия безопасности // Надежность и контроль качества. 1994. № 7.

Software & Systems
DOI: 10.15827/0236-235X.120.690-698

Received 03.04.17
2017, vol. 30, no. 4, pp. 690–698

A METHODICAL APPROACH TO FORMING FUNCTIONAL REQUIREMENTS FOR A COMPUTER ATTACKS PROTECTION SYSTEM FOR AUTOMATED CONTROL SYSTEMS AND ITS SOFTWARE IMPLEMENTATION

E.B. Drobotun [1], *Ph.D. (Engineering), Doctoral Student, drobotun@xakep.ru*

[1] *Military Academy of the Aerospace Defense, Zhigareva St. 50, Tver, 170100, Russian Federation*

Abstract. One of the main stages of development and building of secured automated control systems for various purposes is the stage of forming requirements for the developed automated system including security requirements against computer attacks and other information technology impact.

Effectively developed and reasonable functional requirements for a computer attacks protection system will allow on the one hand providing the necessary level of automated system protection, on the other hand minimizing consumption of computing and human resources of the protected automated system, the amount of which is limited and finite in any automated system.

One of the possible ways to form and prove optimal functional requirements for a computer attacks protection system is using a risk-oriented approach to forming and reasoning of these requirements. The approach includes identifying the severity and probability of possible security threats against the protected automated system.

The article offers a methodical approach to formation of functional requirements for computer attacks protection systems for automated control systems. It is based on a risk assessment of information security threats in the automated system and its safe operation threats.

The application of the proposed approach will allow forming optimal functional requirements for a computer attacks protection system for automated control systems for various purposes. It will help to achieve optimal resource allocation in an automated system to ensure functioning of the computer attacks protection system.

Keywords: automated system, automated system security threat, computer attack, functional requirements, risk analysis.

References

1. Lyaskovsky V.L. *Osnovy proektirovaniya i ekspluatatsii avtomatizirovannykh sistem voennogo naznacheniya* [Fundamentals of Design and Operation of Military Assignment Automated Control Systems]. Moscow, Bauman MSTU Publ., 2016, 188 p.

2. Malyuk A.A., Pazizin S.V., Prigozhin N.S. *Vvedenie v zaschitu informatsii v avtomatizirovannykh sistemakh* [Introduction to Information Protection in Automated Systems]. Moscow, Goryachaya liniya–Telekom Publ., 2001, 148 p.

3. Galatenko V.A. *Standarty informatsionnoy bezopasnosti: kurs lektsy* [Information Security Standards: a Course of Lectures]. V.B. Betelin (Ed.). Moscow, INTUIT.RU Publ., 2006, 264 p.

4. Markov A.S., Tsirlov V.L., Barabanov A.V. *Metody otsenki nesootvetstviya sredstv zashchity informatsii* [Methods for Assessing the Discrepancy of Information Protection Means]. A.S. Markov (Ed.). Moscow, Radio i svyaz Publ., 2012, 192 p.

5. Grishina N.V. The model of a potential intruder on an object of informatization. *Izvestiya UFU. Tekhnicheskie nauki* [News of SFedU. Engineering Science]. 2003, no. 4, vol. 33, pp. 356–358 (in Russ).

6. Zhukov V.G., Zhukova M.N., Stefarov A.P. The model of the violator of access rights in the automated system. *Programmnye produkty i sistemy* [Software & Systems]. 2012, no. 2 (98), pp. 75–78 (in Russ.).

7. Drobotun E.B., Tsvetkov O.V. Building a model of information security threats in an automated control system for critical objects based on the scenarios of the violator's actions. *Programmnye produkty i sistemy* [Software & Systems]. 2016, no. 3 (29), pp. 42–50 (in Russ.).

8. *Common Vulnerability Scoring System*. Available at: http://www.first.org/cvss (accessed March 12, 2017).

9. Nurdinov R.A. Determining the probability of violation of critical properties of the information asset based on the CVSS metrics of the vulnerabilities. *Sovremennye problemy nauki i obrazovaniya* [Modern Problems of Science and Education]. 2014, no. 3. Available at: http://www.science-edukation.ru/pdf/2014/3/344.pdf (accessed March 12, 2017).

10. Belov V., Golyakov A. The terminological base of the theory of security. *Standarty i kachestvo* [Standards and Quality]. 2004, no. 9, pp. 48–51 (in Russ.).

11. Bykov A.A., Porfirev B.N. On the relationship of risk with related concepts and risk management terminology. *Problemy analiza riska* [Problems of risk analysis]. 2013, no. 4, vol. 10, pp. 4–10 (in Russ.).

12. Alpeev A.S. Basic concepts of security. *Nadezhnost i control kachestva* [Reliability and quality control]. 1994, no. 7 (in Russ.).