УДК 004.056.5

А.С. Шабуров, В.Э. Зонова

Пермский национальный исследовательский политехнический университет,
Пермь, Россия

МОДЕЛЬ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Проанализирована проблема информационной безопасности в информационных системах. Перечислены аргументы, обусловливающие возрастающее количество инцидентов информационной безопасности, статистику роста угроз безопасности информации и связанные с активным внедрением информационных технологий. Перечислены наиболее востребованные сферы, требующие обеспечения безопасности. Сформулирована задача защиты объектов критической информационной инфраструктуры. Обеспечение безопасности значимых объектов является составной частью работ по созданию (модернизации), эксплуатации и выводу из эксплуатации значимых объектов. Требования к обеспечению безопасности объектов критической информационной инфраструктуры в ходе разработки, ввода и вывода из эксплуатации подобных объектов являются исходными задачами по защите информации. Перечислены направления для обоснования требований по защите информации, определенные нормативными правовыми документами. Сделан вывод об источниках требований, включаемых в техническое задание на создание системы защиты информации критически важного объекта. Продемонстрирована взаимосвязь моделей, отражающих требования по защите информации, к которым относятся модель угроз безопасности информации и модель системы защиты. Показана целесообразность разработки множества вариантов реализации требований к системам безопасности. Проанализирован процесс формирования требований по защите информации, отражаемых в техническом задании на систему. Определен порядок задания требований, исходя из классификационных признаков объекта критической информационной инфраструктуры. Представлено формальное описание предметной области объекта критической информационной инфраструктуры, основанное на проанализированных данных о нем. Сформулированы решающие правила вывода. Разработана модель представления объекта критической инфраструктуры на основе модели перечисления его уязвимостей и заданных требований. Осуществлена формальная постановка задачи синтеза системы безопасности в соответствии с выбранными критериями.

Ключевые слова: критическая информационная инфраструктура, уровень защищенности, техническое задание, требование по безопасности информации.

A.S. Shaburov, V.E. Zonova

Perm National Research Polytechnic University, Perm, Russian Federation

MODEL IMPLEMENTING REQUIREMENTS FOR THE PROTECTION OF INFORMATION OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

The problem of information security has been analyzed in information systems. The arguments has been listed which is cause an increasing number of information security incidents, statistics on the growth of information security threats and which is relate to the active implementation of information technologies. Most requested areas has been listed which is require protection security in this article. The task has been formulated protection of critical information infrastructure. Protection security significant object is part of the work on creation (modernization), operation and decommissioning of significant object. Requirements protection security of critical information infrastructure are information security tasks during creation, and decommissioning. The directions has been listed for rationale requirements on protection information, which is define of legislation. The conclusion has been drawn about the sources of requirements, which is include in the technical task for the creation of the security subsystem of a significant object. Model relationship has been demonstrated, which is reflect requirements on protection security, which include the model of information security threats and the security system model. The feasibility of developing many options for implementing security systems has been shown. The process of generating information security requirements has been analyzed, which is reflect in the technical task for the system. Requirements specification has been define, based on the classification features of the critical information infrastructure object. Formal description of the subject area of the critical information infrastructure object has been submitted, based on analyzed data about it. Decision rules for withdrawal are formulated. Critical infrastructure facility model has been designed, based on a model for listing its vulnerabilities and specified requirements. Formal formulation of the security system synthesis problem has been implemented to selected criteria.

Keywords: critical information infrastructure, security level, technical task, requirement of information security.

Введение. В настоящее время проблемы безопасности информационных систем приобретают особую актуальность. Это обусловлено возрастающим количеством инцидентов информационной безопасности, статистикой роста угроз безопасности информации, активным внедрением информационных технологий в различных сферах.

Наиболее востребованными в области внедрения информационных технологий, а также обеспечения их безопасности являются такие сферы народно-хозяйственной деятельности, как сфера энергетики, транспорта, связи, здравоохранения, банковская сфера, сферы топливно-энергетического комплекса, атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Необходимость обеспечения защиты подобных систем от кибератак выдвигает новые требования к подобным объектам критической информационной инфраструктуры (КИИ) [1].

При осуществлении работ по созданию (модернизации), эксплуатации и вывода из эксплуатации объектов КИИ обеспечение безопасности является составной и неотъемлемой частью всего комплекса проводимых работ. При этом меры по обеспечению безопасности создаваемых объектов принимаются на всех стадиях (этапах) их жизненного цикла и определяются его категорией [2]. В свою очередь, требования к обеспечению безопасности информации объектов КИИ на всех этапах жизненного цикла являются исходными задачами по защите информации.

Модель реализации требований по защите информации. Определение требований по безопасности объектов КИИ, как и задачи по их защите, возлагаются на собственника объекта КИИ и должны соответствовать категории значимости самого объекта. Уровень категории значимости объекта КИИ также определяется собственником по установленным «Правила категорирования объектов критической информационной инфраструктуры» [3].

Выполнение требований к обеспечению информационной безопасности КИИ, как правило, включает: ключевой набор мер на базе установленной категории значимости объекта КИИ, адаптацию этих мер с угрозами безопасности информации (УБИ), а также меры, обеспечивающие нейтрализацию УБИ с соответствующим уровнем защищенности (УЗ) КИИ. Данные требования включаются в техническое задание (ТЗ) на создание подсистемы безопасности значимого объекта КИИ [4].

Таким образом, в ходе разработки ТЗ на разработку подсистемы безопасности объекта КИИ должны быть обозначены цели, задачи защиты данного объекта, его категория значимости, реализованы организационные и технические меры, этапы и стадии работ и требования к системе защиты, а также перечень нормативных документов по защите объектов КИИ. Внедрение подсистемы безопасности КИИ и системы защиты информации (СЗИ) предполагает разработку модели УБИ. В данной модели должны быть отражены такие задачи, как: выявление источников УБИ, потенциал нарушителей, анализ уязвимостей информационной системы и последствия [5]. Кроме того, в комплекте рабочей документации по защите объекта КИИ требуется ввести описание ее архитектуры; правила эксплуатации; настройку СЗИ. В общем случае реализация требований по защите информации объекта КИИ потребует разработки как модели УБИ, так и модели самой СЗИ (рис. 2).

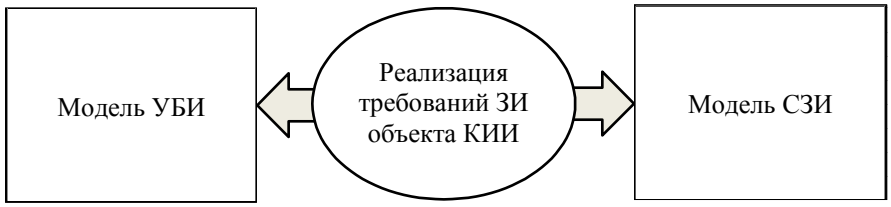

Рис. 1. Взаимосвязь моделей, отражающих требования по защите информации

Как правило, система защиты информации объекта КИИ является сложной системой, на которую возлагается множество функций по обеспечению безопасности функционирования объекта. Противодействие УБИ осуществляется для каждого структурного компонента объекта КИИ и выполняемой функции данного объекта за счет применения различных программных и технических средств защиты информации.

В каждом конкретном случае целесообразно разработать множество вариантов СЗИ, отличающихся структурой, составом, а также таких технико-экономических показателей, как отказоустойчивость, быстродействие, надежность, стоимость, и др. Такого типа показатели довольно часто бывают взаимно противоречивы, что обусловливает целесообразность выбора конкретного решения по защите информации и выбора комплекса средств защиты информации посредством решения оптимизационной задачи, которая требует наличия показателей эффективности защиты информации и выбора соответствующего набора критериев информационной безопасности [6].

Качество подсистемы обеспечения безопасности как составной части объекта КИИ, а также эффективность защиты информации о создаваемой системе безопасности при выполнении работ по ее внедрению в значительной степени зависят от качества реализуемого ТЗ на внедрение СЗИ [7–9].

Несмотря на многочисленные регламентирующие документы в области защиты информации, разработка ТЗ на сложную систему не имеет единого универсального алгоритма и является трудно формализуемой задачей. В том числе это обусловлено широким набором влияющих факторов и неопределенностью влияния множества из них на конечное решение [10]. Кроме того, качество ТЗ во многом определяется квалификацией специалистов, участвующих в его разработке.

Анализ различных объектов КИИ, несмотря на их специфичность, многочисленность и разнообразие, показывает, что каждый

из них обладает рядом общих (типовых) признаков, определяющих необходимость реализации общих (типовых) требований по обеспечению безопасности информации. В то же время специфика конкретных объектов, их ведомственная принадлежность, условия их эксплуатации и характеристики применяемого оборудования во многом обусловливают наличие дополнительных, специальных требований по защите конкретных объектов КИИ. В целом реализация вышеназванных требований предполагает их объединение и сочетание в рамках единого ТЗ на СЗИ объекта КИИ с целью их дальнейшей формализации (рис. 2).

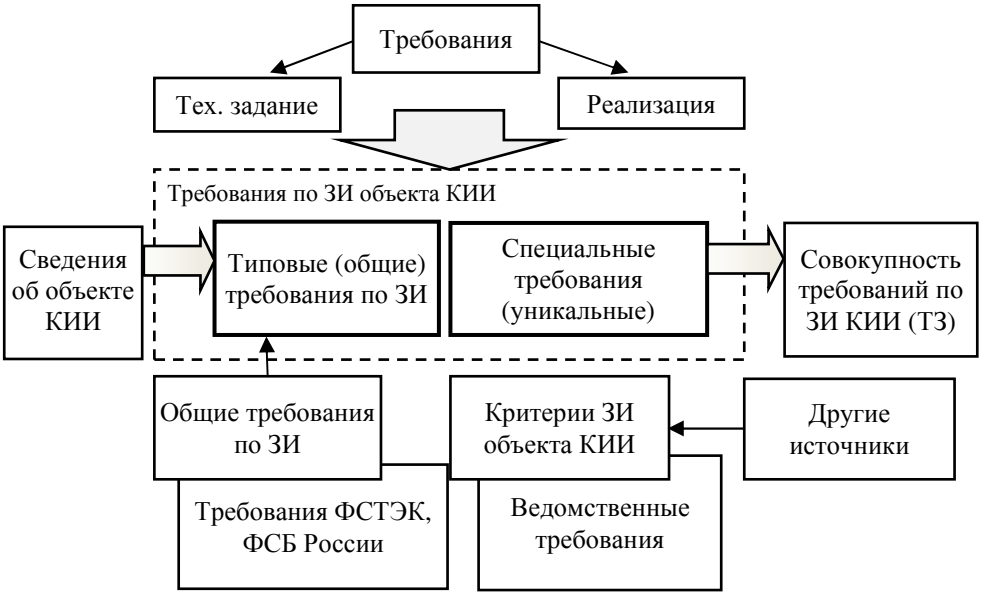

Рис. 2. Составляющие процесса формирования требований по ЗИ объекта КИИ

Формализация формирования общих требований возможна на основе использования соответствия характерных признаков КИИ общим требованиям по обеспечению безопасности информации, а также документов ФСТЭК, ФСБ России, определяющих требования к различным классам и средствам защиты информации [11, 12]. Анализ и реализация общих традиционных подходов позволяют осуществить задачу по созданию СЗИ путем использования накопленного опыта и традиционных схем защиты, уже реализованных на практике, оптимально расходуя временные и информационные ресурсы. Это позволяет сосредоточить основные усилия на разработке специальных (уни-

кальных) требований и создать условия для повышения качества ТЗ. Кроме того, реализация подобного решения представляется целесообразной за счет внедрения системы поддержки принятий решений [13, 14], содержащей информацию об общих (типовых) признаках КИИ, требованиях нормативных документов и вариантах формулировок ТЗ и реализующей алгоритм автоматизированного формирования проекта ТЗ на основе исходных данных.

Таким образом, для определения структуры и содержания базы исходных данных, необходимой для реализации системы поддержки принятия решения по защите объекта КИИ, значение имеет классификация признаков данных объектов и формулировок требований по ЗИ в ТЗ. Данную классификацию целесообразно представить в следующем виде (рис. 3).

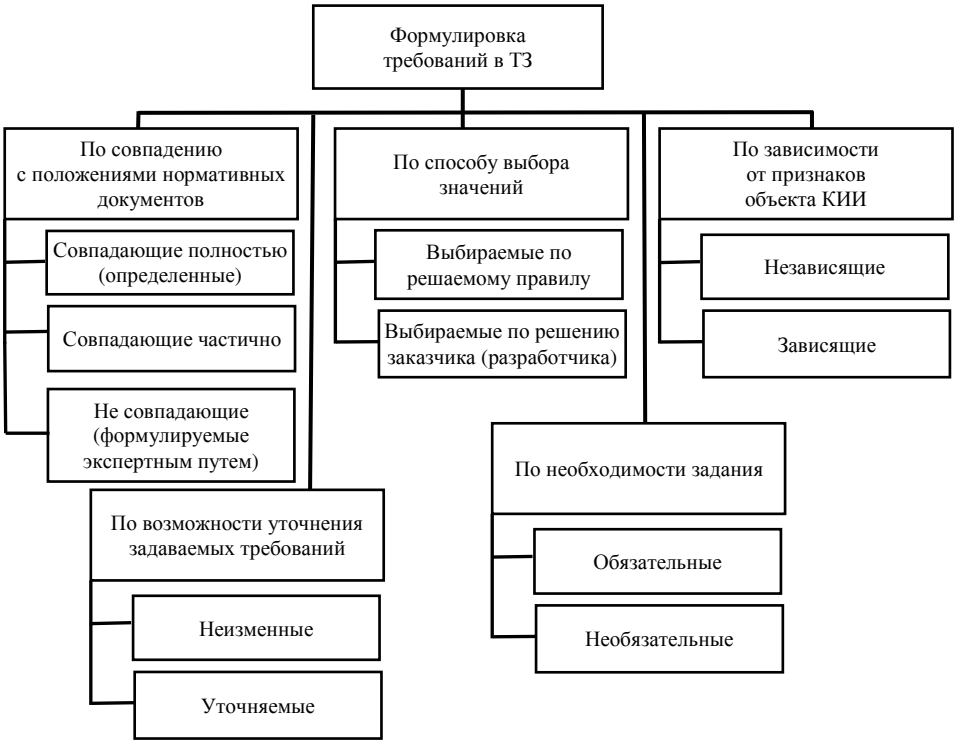

Рис. 3. Классификация формулировок требований по ЗИ объекта КИИ

В качестве классификационных признаков могут быть выбраны те, которые имеют наиболее существенное значение для дальнейшего формального описания предметной области, определения конкретных

признаков объекта КИИ и их допустимых значений, формулировок требований ТЗ соответствия (отношений) между ними в базе данных требований.

Формальное описание предметной области объекта КИИ, основанное на проанализированных данных о нем, позволяет представить ее следующим образом: пусть $\beta = \{\beta^1, \beta^2, ..., \beta^n\}$ – множество признаков объекта КИИ,

$$\beta^1 = \{\beta_1^1, \beta_i^1, ..., \beta_n^1 \,|\, i = \overline{1,n},\ \beta_i^1 = \{Z_{i1}^1, Z_{ip}^1, ..., Z_{ik_i}^1 \,|\, i = \overline{1,k_1}\} \quad (1)$$

множество вспомогательных признаков объекта КИИ, каждый из которых является множеством допустимых значений соответствующего *i*-го первичного признака;

$$\beta^2 = \left\{\beta_1^2, ..., \beta_j^2, ..., \beta_m^1 \,\middle|\, j = \overline{1,m},\ \beta_j^2 = \left\{Z_{j1}^2, ..., Z_{jv}^2, ..., Z_{jk_j}^2 \,\middle|\, v = \overline{1,k_j}\right\}\right\} \quad (2)$$

– это множество производных (вторичных) признаков объекта КИИ, каждый из которых является множеством допустимых значений соответствующего *j*-го производного (вторичного) признака;

L – соответствие допустимых значений признаков КИИ вторичным признакам;

$$S = \{S_1, ..., S_t, ..., S_w \,|\, t = \overline{1,W}\} \quad (3)$$

– множество вторичных формулировок требований к СЗИ в ТЗ на основе анализа связей положений нормативных документов и признаков КИИ;

R – соответствие допустимых значений признаков объекта КИИ сформулированным в ТЗ на создание СЗИ.

Таким образом, описание предметной области защищенного объекта КИИ с учетом введенных обеспечений может быть представлено кортежем:

$$\text{Mod} = <\beta^1, \beta^2, L, S, R>. \quad (4)$$

Тогда модель разработки ТЗ по созданию конкретной создаваемой СЗИ объекта КИИ будет предусматривать последовательное формирование подмножеств:

- первичных признаков создаваемой СЗИ;
- значений первичных признаков создаваемой СЗИ;
- производных (вторичных) признаков создаваемой СЗИ;

– значений производных (вторичных) признаков создаваемой СЗИ;

– формулировок требований к создаваемой СЗИ в ТЗ, соответствующих значениям первичных и производных (вторичных) признаков создаваемой СЗИ.

Например, в качестве первичных признаков можно рассматривать степень конфиденциальности обрабатываемой информации, количество пользователей объекта КИИ, уровень прав доступа к защищаемым ресурсам, в качестве вторичных признаков – класс защищенности от несанкционированного доступа, уровень контроля на соответствие недекларированных возможностей, тип и класс межсетевого экрана и т.п. В общем случае решающее правило $\alpha_{z^2 jv}$, определяющее значение некоторого производного (вторичного) признака, можно представить в виде:

$$\alpha_{z^2 jv} : P_j^2 = Z_{jv}^2 \left| fz_{jv}^2 (Z_{\alpha_0}^1, ..., Z_{yk}^1) = \text{true}, \right. \tag{5}$$

где $f_{c^2 jv}(Z_{\alpha_0}^1, ..., Z_{yk}^1) = Z_{\alpha_0}^1 * ... * Z_{yk}^1$ – логическая функция некоторых переменных множества значений первичных признаков, а $\{Z_{\alpha_0}^1, ..., Z_{yk}^1\}^*$ – логический оператор.

Таким образом, результаты исследования позволяют выработать общий алгоритм формирования ТЗ на объект защиты КИИ на основе содержащейся в базе данных информации.

Следующим этапом реализации требований по ЗИ объекта КИИ является разработка модели СЗИ с учетом уязвимостей конкретного объекта и УБИ объекта КИИ, например, компьютерных атак [15]. Формальная постановка задачи синтеза СЗИ объекта КИИ может быть реализована следующим образом.

Для постановки задачи необходимо представить объект КИИ конечным множеством его уязвимостей $Y = \{y_i\}$:

$$Y = \begin{vmatrix} y_1 \\ \vdots \\ y_i \\ \vdots \\ y_I \end{vmatrix}, \tag{6}$$

где $i = 1 – I$ – номер уязвимости; I – число уязвимостей.

Формальное представление объекта КИИ может служить основой построения математической модели, где абстрактные операторы

преобразования будут заменены математическим описанием реальных процессов функционирования объекта и его составляющих [16, 17]. Однако для многих объектов КИИ со сложной структурой и функциональным многообразием построение такой модели в большинстве случаев невозможно. На практике для выявления уязвимостей объекта КИИ обычно прибегают к экспертным оценкам проектировщиков и опыту специалистов, работающих на этих объектах [18].

Синтез системы обеспечения безопасности критических объектов начинается с формирования модели угроз и построения профиля защиты объекта [19, 20]. Представим конечное множество угроз и способов их реализации $Q = \{q_{jk}\}$ уязвимостям *Y* матрицей-столбцом:

$$Q = \begin{vmatrix} q_{11} \\ \cdot \\ q_{1k} \\ \vdots \\ q_{jk} \\ \cdot \\ q_{jK} \\ \cdot \\ q_{JK} \end{vmatrix} \tag{7}$$

где $j = 1 - J$ – номер потенциальной угрозы; J – число потенциальных угроз; jk – номер способа реализации i-й угрозы; jK – количество способов реализации i-й угрозы.

Если для каждой уязвимости y_i известен перечень угроз ее безопасности и способов их реализации q_{JK}, то профиль защиты объекта КИИ может быть представлен декартовым произведением множеств:

$$Q \times Y = M = \{y_i, q_{JK} / y_i \in Y,\ q_{JK} \in Q\} \tag{8}$$

в виде матрицы *M* бинарных отношений:

$$M = \begin{vmatrix} - & q_{11} & \cdot & q_{1K} & \cdot & q_{jk} & \cdot & q_{jK} & \cdot & q_{JK} \\ y_1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ \cdot & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ y_i & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ \cdot & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ y_l & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}. \tag{9}$$

Матрица *M*, определяющаяся выражением 9, – это формальное представление требований по обеспечению безопасности объекта КИИ.

Эффективность и стоимость множества средств защиты $N = \{n_i\}$ против множества угроз и способов их реализации $Q = \{q_{jk}\}$ представим множеством: $H = \{(P_{ljk}, C_l)\}$

$$H = \begin{vmatrix} - & n_1 & \cdot & \cdot & n_l & \cdot & \cdot & n_L \\ q_{11} & P_{11}, C_1 & - & - & P_{l1}, C_l & - & - & P_{L1}, C_L \\ \cdot & P_{11k}, C_1 & P_{21k}, C_2 & - & - & - & - & - \\ q_{1K} & P_{11K}, C_1 & - & - & P_{l1K}, C_l & - & - & - \\ \cdot & P_{12k}, C_1 & - & - & - & - & - & P_{L2k}, C_L \\ q_{jk} & P_{1jk}, C_1 & P_{2jk}, C_2 & - & - & - & - & P_{Ljk}, C_L \\ \cdot & P_{1jk}, C_1 & P_{2jk}, C_2 & - & P_{ljk}, C_l & - & - & - \\ q_{JK} & P_{1JK}, C_1 & - & - & - & - & - & P_{LJK}, C_L \end{vmatrix}, \qquad (10)$$

где $l = 1 - L$ – номер средства защиты; L – количество средств защиты; P_{ljk} – эффективность средства защиты – вероятности нейтрализации j-го способа k-й угрозы; C_l – стоимость l-го средства защиты.

Декартово произведение множеств M и H формирует множество:

$$S = M \times H = \left\{ \frac{y_i, q_{jk}, P_{ljk}, C_l}{y_i} \in Y,\ q_{jk} \in Q,\ P_{ljk} \in H,\ C_l \in H \right\}, \qquad (11)$$

где каждой уязвимости y_i сопоставлено множество угроз и способов их реализации q_{jk} и множество средств защиты и их стоимости $H = \{P_{ljk}, C_l\}$.

Множество S можно представить трехмерной матрицей, содержащей всю информацию, необходимую для формальной постановки задач синтеза системы безопасности в соответствии с выбранными критериями. При этом единым критерием оценки эффективности системы безопасности и его составляющих служит величина риска нарушения безопасности хотя бы одной уязвимости объекта – R_i.

В общем случае величина риска R нарушения безопасности критического объекта – это функция от значений рисков $\{R_i\}$ нарушения безопасности множества его уязвимостей $R = f\{R_i\} \forall y_i \in Y$ и неопределенностей, связанных с недостатком и недостаточностью информации, представленной множествами Y, Q и M.

Заключительным этапом синтеза системы защиты информации является выбор по критериям R и R_i состава средств защиты (композиции) для каждой уязвимости:

$$N_{yi} = \{n_{li}\} \subset N_y \subset N \forall y_i \in Y. \qquad (12)$$

Этот выбор может быть представлен двумя постановками задач синтеза композиции СЗИ объекта КИИ.

Первая постановка задачи может быть сформулирована следующим образом: определить множество композиций $N_y = \{N_{yi}\} \subset N$, обеспечивающих риски нарушения безопасности критической инфраструктуры R и его уязвимостей $\{R_i\}$ не больше допустимых $R \le R_{\text{доп}}$ и $R_i \le R_{\text{доп}} \forall y_i \in Y$ при минимуме стоимости средств защиты системы безопасности $\min C_Y = \sum \min C_i$. Задача решается последовательным выбором композиций N_{yi} для всех уязвимостей $\forall y_i \in Y$ по критерию $\min C_i$ и формированием матрицы $S_{\text{opt}C}$ состава системы защиты информации:

$$S_{\text{opt}C} = \begin{vmatrix} - & n_1 & \cdot & n_l & \cdot & n_L \\ y_1 & 1 & 0 & 1 & 1 & 0 \\ \cdot & 1 & 1 & 1 & 1 & 0 \\ y_i & 1 & 1 & 1 & 0 & 0 \\ \cdot & 1 & 0 & 0 & 1 & 1 \\ y_I & 1 & 0 & 0 & 1 & 0 \end{vmatrix}. \qquad (13)$$

Вторая постановка может быть сформулирована следующим образом: определить множество композиций $N_y = \{N_{yi}\} \subset N,$, обеспечивающих равный минимальный уровень риска нарушения безопасности критического объекта, можно как $\min R_i \forall y_i \in Y$ при заданных расходах $C_{\text{доп}}$. Задача заключается в распределении средств $C_{\text{доп}}$, выделенных на обеспечение безопасности критической инфраструктуры между уязвимостями по критерию равенства минимумов рисков нарушения их безопасности, и преобразовании матрицы S в матрицу средств защиты системы безопасности критического объекта при ограничении их суммарной стоимости:

$$S_{\text{opt}C_{\text{доп}}} = \begin{vmatrix} - & n_1 & \cdot & n_l & \cdot & n_L \\ y_1 & 1 & 0 & 1 & 1 & 0 \\ \cdot & 1 & 1 & 1 & 1 & 0 \\ y_i & 1 & 1 & 1 & 0 & 0 \\ \cdot & 1 & 0 & 0 & 1 & 1 \\ y_I & 1 & 0 & 0 & 1 & 0 \end{vmatrix}. \qquad (14)$$

Обе постановки задачи синтеза композиций СЗИ объекта КИИ предполагают наличие методов количественной оценки рисков нарушения безопасности R и его составляющих R_i [14].

Выводы. Проведенный анализ предметной области позволяет рассмотреть порядок формирования ТЗ на создание подсистем обеспечения информационной безопасности объектов КИИ как с точки зрения задания типовых (общих) требований по защите информации, так и в части, касающейся специальных, (уникальных) требований. Предлагаемый подход на основе модели задания требований по защите информации позволяет выработать общий алгоритм автоматизированного формирования ТЗ. Предложенная модель позволяет сократить время, необходимое заказчику или эксперту на разработку ТЗ в части требований по защите информации, а также повысить качество самого ТЗ, а также качество создаваемой на его основе системы защиты информации. Дальнейшее направление развития научного исследования предполагает разработку и внедрение интеллектуальных алгоритмов поддержки принятия решений заказчика (эксперта) для формирования ТЗ. Кроме того, представленные методы формального описания требований объектов КИИ и постановки задач обеспечения их безопасности могут быть реализованы на примере различных критических инфраструктур, что позволяет с единых теоретических позиций разрабатывать и применять универсальный подход определения требований к системам защиты информации объектов КИИ.

Библиографический список

1. Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» // Доступ из справ.-правовой системы КонсультантПлюс.

2. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» // Доступ из справ.-правовой системы КонсультантПлюс.

3. Постановление Правительства Российской Федерации от 8 февраля 2019 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // Доступ из справ.-правовой системы КонсультантПлюс.

4. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // Доступ из справ.-правовой системы КонсультантПлюс.

5. Шабуров А.С., Зонова В.Э., Рыжук Н.С. Защита критической информационной инфраструктуры в соответствии с требованиями по обеспечению безопасности информации // Инновационные технологии: теория, инструменты, практика: материалы X Междунар. интернет-конф. молод. ученых, аспир., студ., 20.11–31.12.2018. – Пермь: Изд-во Перм. нац. исследов. политехн. ун-та, 2019. – С. 397–403.

6. Шабуров А.С., Миронова А.А. О повышении эффективности защиты персональных данных в информационных системах открытого типа // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2015. – № 16. – С. 106–117.

7. Муравник В.Б., Захаренков А.И., Добродеев А.Ю. Некоторые предложения по подходу и порядку реализации политики и стратегии импортозамещения в интересах национальной безопасности и укрепления обороноспособности Российской Федерации // Вопросы кибербезопасности. – 2016. – № 1(14). – С. 2–8.

8. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении / под общ. ред. С.Ф. Боева; ввод. слово А.И. Смирнова, А.Г. Тормасова; ввод. статья И.А. Каляева. – Иннополис: Изд. дом «Афина», 2017. – 440 с.

9. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. – 2013. – № 1(1). – С. 17–27.

10. Бибашов С.А. Модель формирования требований по защите информации к создаваемым автоматизированным системам в защищенном исполнении // Вопросы кибербезопасности. – 2017. – № 5(23). – С. 83–90.

11. Барабанов А.В., Марков А.С., Цирлов В.Л. Оценка соответствия средств защиты информации «Общим критериям» // Информационные технологии. – 2015. – Т. 21. – № 4. – С. 264–270.

12. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. – М.: Радио и связь, 2012. – 192 с.

13. Исаев Г.Н. Проектирование информационных систем: учеб. пособие. – М.: Омега-Л, 2013. – 424 с.

14. Микони С.В. Теория принятия управленческих решений: учеб. пособие. – СПб.: Лань, 2015. – 448 с.

15. Шабуров А.С. О разработке модели обнаружения компьютерных атак на объекты критической информационной инфраструктуры // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2018. – № 26. – С. 199–213.

16. Хуснулин Р.Г. Использование технического задания на защиту информации при разработке интегрированной автоматизированной системы управления в защищенном исполнении // Фундаментальные и прикладные исследования в современном мире: материалы междунар. науч.-практ. конф. – СПб.: Информац. издат. учеб.-науч. центр «Стратегия будущего», 2013. – № 2. – С. 71–78.

17. Орлова Ю.А. Алгоритмическое обеспечение анализа текста технического задания и построения моделей программного обеспечения // Известия Волгоград. гос. техн. ун-та. Сер. Актуальные проблемы управления, вычислительной техники и информатики в технических системах: межвуз. сб. науч. ст. – Волгоград, 2010. – Вып. 8, № 6(66). – С. 68–72.

18. Цыгичко В.Н., Черешкин Д.С., Смолян Г.Л. Безопасность критических инфраструктур. – М.: ЛЕНАНД, 2019. – 200 с.

19. Farah T., Trajkovic L. Anonym: A tool for anonymization of the Internet traffic // IEEE 2013 International Conference on Cybernetics (CYBCONF). – 2013. – P. 261–266.

20. Orebaugh Angela, Gilbert Ramirez, Jay Beale. Wireshark & Ethereal network protocol analyzer toolkit. – Elsevier, 2006.

References

1. Federal'nyi zakon ot 26.07.2017 № 187 «O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii» [Federal Law of July 26, 2017 No. 187 “On the Security of Critical Information In-

frastructure of the Russian Federation"]. Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

2. Prikaz FSTEK Rossii ot 21 dekabria 2017 g. № 235 «Ob utverzhdenii trebovanii k sozdaniiu sistem bezopasnosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii i obespecheniiu ikh funktsionirovaniia» [Order of the FSTEC of Russia dated December 21, 2017 No. 235 "On approval of requirements for the creation of security systems for significant objects of critical information infrastructure of the Russian Federation and ensuring their functioning"]. Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

3. Postanovlenie Pravitel'stva Rossiiskoi Federatsii ot 8 fevralia 2019 g. № 127 «Ob utverzhdenii Pravil kategorirovaniia ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii, a takzhe perechnia pokazatelei kriteriev znachimosti ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii i ikh znachenii» [Decree of the Government of the Russian Federation of February 8, 2019 No. 127 "On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the importance of objects of critical information infrastructure of the Russian Federation and their values"] Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

4. Prikaz FSTEK Rossii ot 25 dekabria 2017 g. № 239 «Ob utverzhdenii trebovanii po obespecheniiu bezopasnosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii» [Order of the FSTEC of Russia of December 25, 2017 No. 239 "On approval of requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation"]. Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

5. Shaburov A.S., Zonova V.E., Ryzhuk N.S. Zashchita kriticheskoi informatsionnoi infrastruktury v sootvetstvii s trebovaniiami po obespecheniiu bezopasnosti informatsii [Protection of critical information infrastructure in accordance with information security requirements]. *Innovatsionnye tekhnologii: teoriia, instrumenty, praktika. Materialy X Mezhdunarodnoi internet-konferentsii molodykh uchenykh, aspirantov, studentov*, 20 November - 31 December 2018. Perm': Permskii natsional'nyi issledovatel'skii politekhnicheskii universitet, 2019, pp. 397-403.

6. Shaburov A.S., Mironova A.A. O povyshenii effektivnosti zashchity personal'nykh dannykh v informatsionnykh sistemakh otkrytogo tipa [On improving the efficiency of personal data protection in open-type information systems]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2015, no. 16, pp. 106-117.

7. Muravnik V.B., Zakharenkov A.I., Dobrodeev A.Iu. Nekotorye predlozheniia po podkhodu i poriadku realizatsii politiki i strategii importozameshcheniia v interesakh natsional'noi bezopasnosti i ukrepleniia oboronosposobnosti Rossiiskoi Federatsii [Some suggestions on the approach and procedure for implementing the policy and strategy of import substitution in the interests of national security and strengthening the defense capability of the Russian Federation]. *Voprosy kiberbezopasnosti*, 2016, no. 1(14), pp. 2-8.

8. Petrenko S.A., Stupin D.D. Natsional'naia sistema rannego preduprezhdeniia o komp'iuternom napadenii [National Computer Attack Early Warning System]. Ed. S.F. Boeva, vvodnye slova A.I. Smirnova, A.G. Tormasova, vvodnaia stat'ia I.A. Kaliaeva. Innopolis: Izdatel'skii dom "Afina", 2017. 440 p.

9. Chobanian V.A., Shakhalov I.Iu. Analiz i sintez trebovanii k sistemam bezopasnosti ob"ektov kriticheskoi informatsionnoi infrastruktury [Analysis and synthesis of requirements for security systems of critical information infrastructure facilities]. *Voprosy kiberbezopasnosti*, 2013, no. 1(1), pp. 17-27.

10. Bibashov S.A. Model' formirovaniia trebovanii po zashchite informatsii k sozdavaemym avtomatizirovannym sistemam v zashchishchennom ispolnenii [A model for the formation of requirements for the protection of information for created automated systems in a secure execution]. *Voprosy kiberbezopasnosti*, 2017, no. 5(23), pp. 83-90.

11. Barabanov A.V., Markov A.S., Tsirlov V.L. Otsenka sootvetstviia sredstv zashchity informatsii "Obshchim kriteriiam" [Assessment of compliance of information protection means with "General Criteria"]. *Informatsionnye tekhnologii*, 2015, vol. 21, no. 4, pp. 264-270.

12. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody otsenki nesootvetstviia sredstv zashchity informatsii [Methods for assessing noncompliance of information security tools]. Moscow: Radio i sviaz', 2012. 192 p.

13. Isaev G.N. Proektirovanie informatsionnykh sistem [Designing information systems]. Moscow: Omega-L, 2013. 424 p.

14. Mikoni S.V. Teoriia priniatiia upravlencheskikh reshenii [Theory of managerial decision making]. Saint Petersburg: Lan', 2015. 448 p.

15. Shaburov A.S. O razrabotke modeli obnaruzheniia komp'iuternykh atak na ob"ekty kriticheskoi informatsionnoi infrastruktury [On the development of a model for detecting computer attacks on objects of critical information infrastructure]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2018, no. 26, pp. 199-213.

16. Khusnulin R.G. Ispol'zovanie tekhnicheskogo zadaniia na zashchitu informatsii pri razrabotke integrirovannoi avtomatizirovannoi sistemy upravleniia v zashchishchennom ispolnenii [The use of technical specifications for information security in the development of an integrated automated control system in a secure execution]. *Fundamental'nye i prikladnye issledovaniia v sovremennom mire. Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii*. Saint Petersburg: Informatsionnyi izdatel'skii uchebno-nauchnyi tsentr «Strategiia budushchego», 2013, no. 2, pp. 71-78.

17. Orlova Iu.A. Algoritmicheskoe obespechenie analiza teksta tekhnicheskogo zadaniia i postroeniia modelei programmnogo obespecheniia [Algorithmic support for the analysis of the text of the technical specifications and the construction of software models]. *Izvestiia Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. Aktual'nye problemy upravleniia, vychislitel'noi tekhniki i informatiki v tekhnicheskikh sistemakh: mezhvuzovskii sbornik nauchnykh statei*. Volgograd, 2010, iss. 8, no. 6(66), pp. 68-72.

18. Tsygichko V.N., Chereshkin D.S., Smolian G.L. Bezopasnost' kriticheskikh infrastruktur [Critical Infrastructure Security]. Moscow: LENAND, 2019. 200 p.

19. Farah T., Trajkovic L. Anonym: A tool for anonymization of the Internet traffic. *IEEE 2013 International Conference on Cybernetics (CYBCONF)*, 2013, pp. 261-266.

20. Orebaugh Angela, Gilbert Ramirez, Jay Beale. Wireshark & Ethereal network protocol analyzer toolkit. Elsevier, 2006.

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Зонова Виктория Эдуардовна (Пермь, Россия) – студентка Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: us277@mail.ru).

About the authors

Shaburov Andrey Sergeevich, (Perm, Russian Federation) is a Ph.D in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Zonova Victoriya Eduardovna (Perm, Russian Federation) is a Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: us277@mail.ru).

Получено 30.10.2019