МОДЕЛЬ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ К СОЗДАВАЕМЫМ АВТОМАТИЗИРОВАННЫМ СИСТЕМАМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Бибашов С.А.[1]

В статье представлены результаты анализа и формальное описание предметной области, охватывающей порядок создания автоматизированных систем в защищенном исполнении и формирования тактико–технических заданий по вопросам защиты информации. Проведен анализ современных автоматизированных систем в защищенном исполнении. Даны классификации признаков защищенных автоматизированных систем и нормативных формулировок требований в современных нормативных документах. Указаны причины недостатков имеющихся требований к автоматизированным системам. Представлена концептуальная формальная модель разработки тактико–технического задания к разрабатываемой автоматизированной системе в защищенном исполнении. Разработан общий алгоритм автоматизированного формирования тактико–технического задания и основные требования к структуре и содержанию базы данных, необходимой для его программной реализации. Показано, что предлагаемые решения позволяют сократить время на разработку тактико–технических заданий при повышении качества создаваемой на его основе автоматизированной системы в защищенном исполнении.

Ключевые слова: *тактико–техническое задание, опытно–конструкторская работа, защита информации, база данных, проектирование.*

DOI: 10.21681/2311-3456-2017-5-83-90

Введение

В современных условиях потребности органов военного управления, воинских частей и организаций Вооруженных Сил Российской Федерации в различных автоматизированных системах, предназначенных для обработки информации ограниченного доступа (АСЗИ), неуклонно возрастают. При этом независимо от функционального предназначения АСЗИ неотъемлемой составной частью каждой из них должна являться система защита информации.

Качество системы защиты информации как составной части АСЗИ, а также эффективность защиты сведений о создаваемой системе при выполнении опытно-конструкторской работы (ОКР), в значительной степени зависят от качества соответствующего тактико-технического задания (ТТЗ) [1-4].

Анализ ТТЗ на создание АСЗИ [5, 6] показывает, что при разработке данной категории документов, являющихся неотъемлемой частью государственных контрактов на выполнение ОКР [1, 7], допускается значительное количество существенных ошибок и недоработок, приводящих к необходимости внесения соответствующих изменений и увеличению времени согласования ТТЗ, а также создающих предпосылки разработки средств и систем защиты информации, не в полной мере соответствующих требованиям нормативных документов.

Снижение качества ТТЗ объясняется следующими основными причинами:

- многочисленностью и несогласованностью в отдельных случаях нормативных документов по вопросам создания АСЗИ;
- усложнением создаваемых АСЗИ и расширением их функционального предназначения;
- невозможностью задания адекватных и достаточных требований по защите информации только лишь на основе «традиционных» нормативных документов, не учитывающих специфику современных (перспективных) информационных технологий и средств;
- отсутствием у ответственных должностных лиц достаточного времени на качественную разработку, рассмотрение и согласование ТТЗ.

В настоящей статье приводятся результаты исследований предметной области и предлагается модель формирования ТТЗ на АСЗИ по вопросам защиты информации, использование которой может повысить качество разрабатываемых ТТЗ.

1 Бибашов Сергей Александрович, Военная академия Ракетных войск стратегического назначения имени Петра Великого, Москва, Россия, E-mail: sbma82@mail.ru

Постановка задачи

Цель исследования - разработка предложений по повышению качества систем защиты информации создаваемых АСЗИ за счет улучшения качества ТТЗ в условиях ограниченности временных ресурсов.

Для достижения поставленной цели необходимо:

- провести анализ предметной области, охватывающей порядок создания АСЗИ и формирования ТТЗ в части касающейся требований по защите информации;
- разработать модель формализованного создания ТТЗ, позволяющую сократить время на формирование требований по защите информации при улучшении качества ТТЗ.

Анализ предметной области

Анализ различных типов АСЗИ, а также положений как обязательных, так и рекомендуемых к применению при их создании (эксплуатации) нормативных документов [5, 8, 9] показал, что:

- несмотря на многочисленность и специфичность автоматизированных систем, каждая из них обладает рядом общих (типовых) и существенных признаков, определяющих необходимость реализации конкретных требований нормативных документов в рамках создания (эксплуатации) соответствующей системы защиты информации;
- наряду с общими (типовыми) признаками любая АСЗИ имеет специфические признаки, для которых требования в нормативных документах могут отсутствовать или определяться в общем виде (не конкретно);
- общие (типовые) признаки АСЗИ, их допустимые (возможные) значения, а также требования нормативных документов по защите информации могут быть обобщены, структурированы (классифицированы) и связаны соответствующими отношениями;
- требования (положения) нормативных документов, связанные с общими (типовыми) признаками АСЗИ, как правило, не эквивалентны на синтаксическом уровне семантически соответствующим им формулировкам в ТТЗ [10]. При этом формулировки ТТЗ как составной части государственного контракта с одной стороны должны быть точными и не противоречащими положениям нормативных документов, с другой стороны они не должны ограничивать разработчика системы в поиске и реализации наиболее эффективных решений;
- разработка ТТЗ, несмотря на многочисленность регламентирующих данную область нормативных документов, в общем случае, не имеет единого универсального алгоритма и является трудно формализуемой в полном объеме задачей, в том числе из-за широкого набора влияющих факторов и априорной неопределенности множества из них. Качество ТТЗ во многом зависит от квалификации и опыта участвующих в его разработке (согласовании) должностных лиц и находящихся в их распоряжении ресурсов (информационных, временных, методических и др.);
- процесс разработки ТТЗ условно может быть разделен на этапы формирования общих (типовых) и специальных (уникальных) для создаваемой АСЗИ требований. Тогда время формирования проекта ТТЗ $T_{ТТЗ} = T_{ОБЩ} + T_{СП}$, *где* $T_{ОБЩ}$, $T_{СП}$ - время разработки общих (типовых) и специальных (уникальных) требований соответственно (рис. 1). При этом формализация этапа формирования

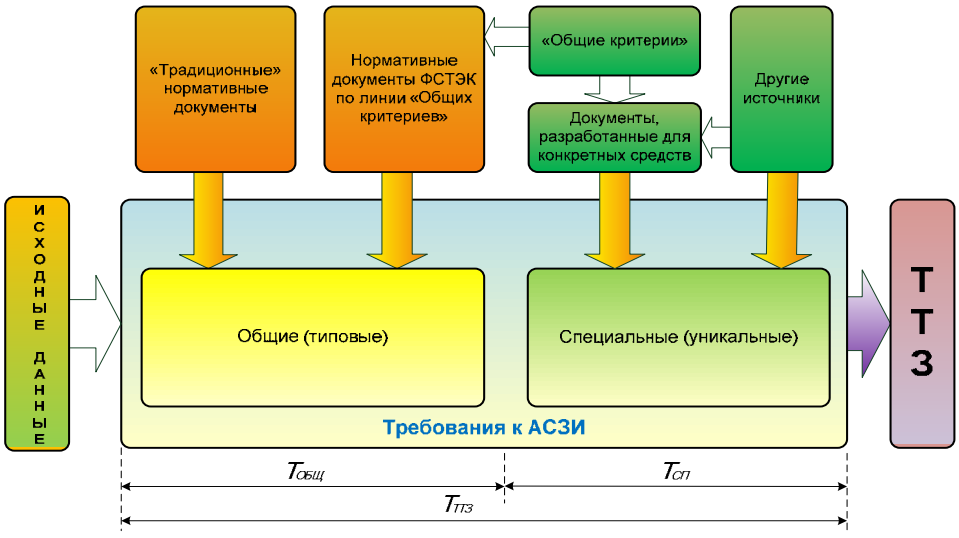

***Рис. 1**. Составляющие процесса формирования требований по защите информации к создаваемым АСЗИ в ТТЗ*

общих (типовых) требований возможна на основе использования соответствий общих (типовых) признаков АСЗИ требованиям «традиционных» нормативных документов, а также документов ФСТЭК России, разработанных по линии «Общих критериев» и определяющих требования к различным средствам защиты информации [9, 11]. Это позволит увеличить количество имеющихся у должностных лиц временных и информационных ресурсов, сосредоточить их основные усилия на разработке специальных (уникальных) требований и создать условия для повышения качества ТТЗ;

- реализация предлагаемого решения представляется целеобразным за счет внедрения системы (элементов системы) поддержки принятий решений [12, 13], содержащей информацию об общих (типовых) признаках АСЗИ, требованиях нормативных документов и вариантах формулировок ТТЗ, и реализующей алгоритм автоматизированного формирования проекта технического задания на основе исходных данных.

С учетом изложенного, для определения структуры и содержания базы данных, необходимой для реализации системы (элемента системы) поддержки принятия решения заказчика, важное значение имеет классификация признаков АСЗИ и формулировок (требований) в ТТЗ, которая может быть представлена в следующем виде (рис. 2).

В качестве классификационных признаков выбраны те, которые имеют наиболее существенное значение для дальнейшего формального описания предметной области, определения конкретных признаков АСЗИ и их допустимых (возможных) значений, формулировок (требований) ТТЗ и соответствия (отношений) между ними в базе данных.

Формальное описание предметной области, основанное на сформулированных ранее выводах и представленной на рисунке 1 классификации, может быть представлено с использованием следующих обозначений:

$P = \{P^1, P^2\}$ – множество признаков АСЗИ;

$$P^1 = \left\{P_1^1, \dots, P_i^1, \dots, P_n^1 | i = \overline{1,n}, P_i^1 = \right.$$
$$\left. = \left\{Z_{i_1}^1, \dots, Z_{i_p}^1, \dots, Z_{i_{ki}}^1 | p = \overline{1,ki}\right\}\right\}$$ – множество возможных первичных признаков АСЗИ, каждый из которых является множеством допустимых

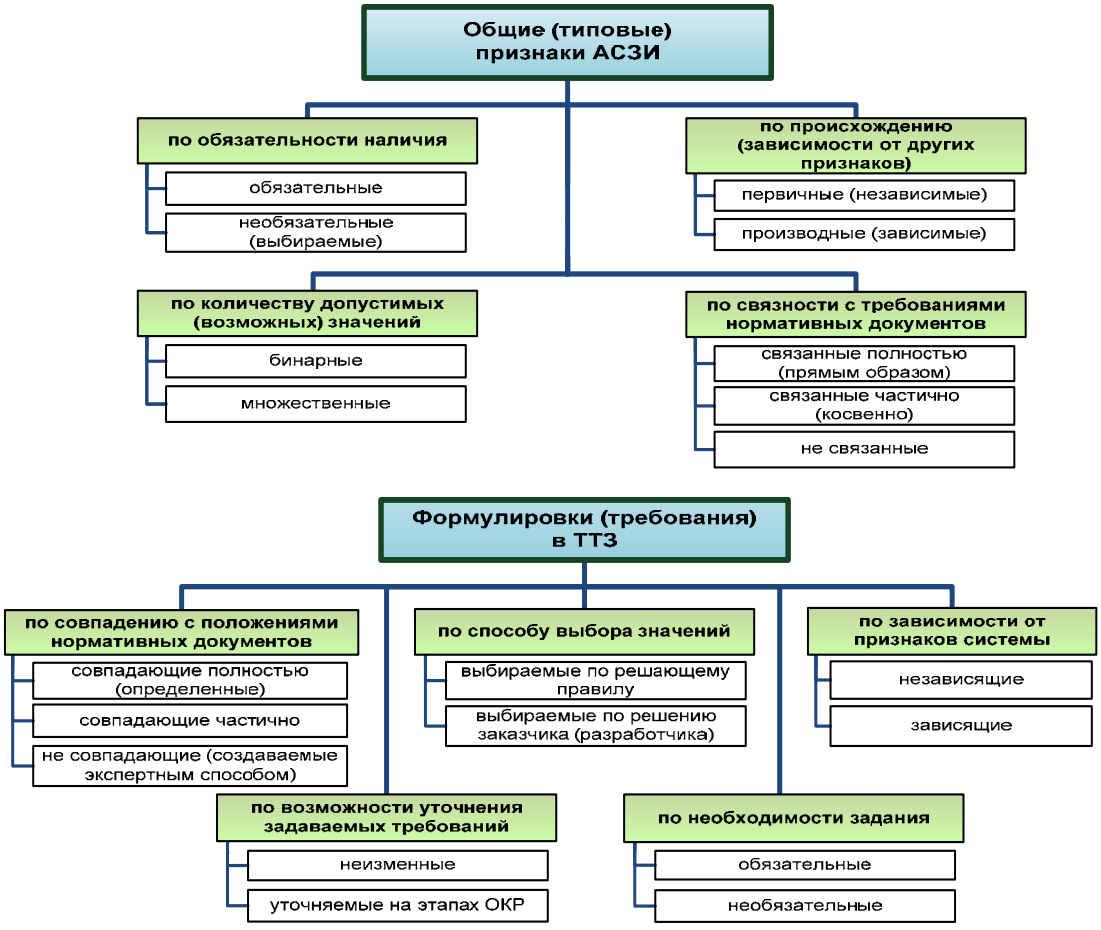

***Рис. 2**. Классификация признаков АСЗИ и формулировок (требований) в ТТЗ*

(возможных) значений соответствующего *i*-го первичного признака;

$P^2 = \left\{P_1^2, \dots, P_j^2, \dots, P_m^2 | j = \overline{1,m}, P_j^2 = \right.$

$\left. = \left\{Z_{j_1}^2, \dots, Z_{j_v}^2, \dots, Z_{j_{kj}}^2 | v = \overline{1,kj}\right\}\right\}$ – множество производных (вторичных) признаков АСЗИ, каждый из которых является множеством допустимых (возможных) значений соответствующего *j*-го производного (вторичного) признака;

Ψ – соответствие допустимых (возможных) значений первичных признаков производным (вторичным) признакам;

$\Phi = \{\phi_1, \dots, \phi_g, \dots, \phi_w | g = \overline{1,w}\}$ – множество возможных формулировок требований к АСЗИ в ТТЗ, составленных на основе анализа связей положений нормативных документов и признаков АСЗИ;

Θ – соответствие допустимых (возможных) значений признаков АСЗИ формулировкам в ТТЗ.

Таким образом, описание предметной области с учетом введенных обозначений может быть представлено кортежем следующего вида:

$$Mod = \langle P^1, P^2, \Psi, \Theta, \Phi \rangle.$$

Тогда модель разработки ТТЗ по созданию конкретной АСЗИ будет предусматривать последовательное формирование подмножеств:

первичных признаков конкретной (создаваемой) АСЗИ P^{1^*};

значений первичных признаков конкретной (создаваемой) АСЗИ Z^{1^*};

производных (вторичных) признаков конкретной (создаваемой) АСЗИ P^{2^*};

значений производных (вторичных) признаков конкретной (создаваемой) АСЗИ Z^{2^*};

формулировок требований к создаваемой АСЗИ в ТТЗ Φ^*, соответствующих значениям первичных и производных (вторичных) признаков конкретной (создаваемой) АСЗИ.

Графическая интерпретация формального описания предметной области и модели разработки ТТЗ представлена на рис. 3.

В качестве первичных признаков P^1 можно отметить максимальную степень секретности (конфиденциальности) обрабатываемой информации, количество пользователей, права доступа к защищаемым ресурсам и т.д., в качестве вторичных P^2 – класс защищенности АСЗИ от несанкционированного доступа, уровень контроля отсутствия недекларированных возможностей программного обеспечения, тип межсетевого экрана, класс защиты межсетевого экрана и т.д.

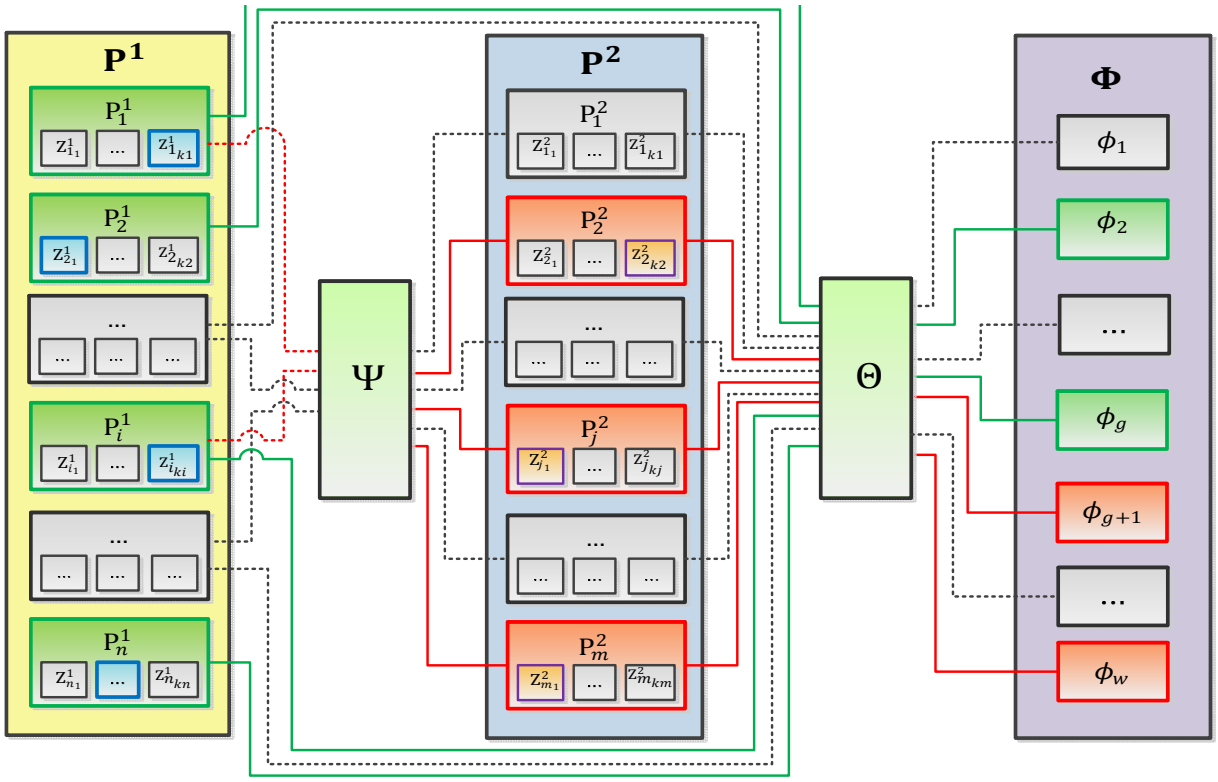

Рис. 3. *Графическая интерпретация формального описания предметной области и модели разработки ТТЗ*

Таблица 1.
Примеры отношений первичных и производных (вторичных) признаков АСЗИ

Первичные признаки			Производный (вторичный) признак
максимальная степень секретности обрабатываемой информации	количество пользователей	права доступа	класс защищенности АС от НСД
особой важности	много	различные	1А
совершенно секретно	много	различные	1Б
секретно	много	различные	1В
особой важности	много	равные	2А
совершенно секретно	много	равные	2А
секретно	много	равные	2А
особой важности	один	-	3А
совершенно секретно	один	-	3А
секретно	один	-	3А

Примеры отношений (соответствий) первичных и производных (вторичных) признаков представлены в табл. 1.

Состав первичных признаков P^{1^*} и их значений Z^{1^*} конкретной (создаваемой) АСЗИ зависит от исходных данных сформированных заказчиком.

Перечень производных (вторичных) признаков P^{2^*} конкретной (создаваемой) АСЗИ зависит от сочетания различных первичных признаков P^{1^*} и их значений Z^{1^*}, а значения Z^{2^*} в общем случае могут определяться либо по выбору заказчика (эксперта), либо в результате выполнения решающего правила.

В общем случае решающее правило $a_{Z^z_{j_v}}$, определяющее значение некоторого производного (вторичного) признака, можно представить в виде:

$$a_{Z^z_{j_v}} : P^2_j = Z^2_{j_v} | f_{Z^z_{j_v}}\left(Z^1_{x_o}, \dots, Z^1_{y_k}\right) = true,$$

где $f_{Z^z_{j_v}}\left(Z^1_{x_o}, \dots, Z^1_{y_k}\right) = Z^1_{x_o} * \dots * Z^1_{y_k}$ – логическая функция некоторых переменных множества значений первичных признаков $\left\{Z^1_{x_o}, \dots, Z^1_{y_k}\right\}$, $*$ - логический оператор.

Так, в соответствии с таблицей 1 значение «1Б» производного (вторичного) признака «класс защищенности АС от НСД» будет истинным (выбранным) тогда и только тогда, когда одновременно будет истинна конъюнкция значений «совершенно секретно», «много», «различные» соответствующих первичных признаков. Вместе с тем для классов защищенности «2А» и «3А» определяющими будут значения первичных признаков «права доступа» и (или) «количество пользователей» независимо от максимальной степени секретности обрабатываемой информации.

Таким образом, результаты исследования позволяют выработать общий алгоритм формирования ТТЗ на основе содержащейся в базе данных информации.

Алгоритм автоматизированного формирования ТТЗ и общие требования к базе данных

Алгоритм формирования проекта ТТЗ в части требований по защите информации в общем виде можно представить следующими образом:

1. Изучение исходных данных для создания АСЗИ;

2. Определение и выборка из множества P^1 перечня первичных признаков P^{1^*} создаваемой АСЗИ;

3. Выбор значения для каждого первичного признака P^{1^*} и формирование множества Z^{1^*};

4. Определение и выборка из множества P^2 перечня производных (вторичных) признаков P^{2^*} по соответствию Ψ;

5. Выбор значения для каждого производного (вторичного) признака P^{2^*} и формирование множества Z^{2^*} на основании решающих правил или по решению заказчика (эксперта);

6. Определение из множества Φ по соответствию Θ формулировок Φ^* для создаваемой АСЗИ;

7. Формирование проекта ТТЗ, включающего множество формулировок $\Phi^{\ddagger}$.

Далее сформированный проект ТТЗ может быть дополнен необходимыми другими, в том числе специфическими (уникальными) требованиями.

Кроме того, необходимо учитывать следующие особенности:

- проект ТТЗ целесообразно формировать на основе шаблона, соответствующего требованиям государственных стандартов, для чего требуется задание отношений (соответствий) формулировок Φ позициям (закладкам) в шаблоне;
- для возможности выбора значений признаков по решению заказчика необходима реализация интерактивного режима работы программного обеспечения, что предполагает наличие в базе данных контрольных вопросов, соответствующих конкретным признакам (значениям признаков).
- С учетом полученных результатов база данных поддержки принятия решений заказчика (эксперта) должна содержать следующие основные сущности (таблицы):
- признаки АСЗИ, содержащая такие экземпляры сущностей как первичные и производные (вторичные) признаки;
- первичные и производные (вторичные) признаки (раздельно), каждая из которых в качестве экземпляров сущностей содержит множество допустимых (возможных) значений;
- контрольные вопросы для обеспечения интерактивного режима работы программного обеспечения и возможности выбора значений признаков заказчиком (экспертом);
- формулировки требований ТТЗ;
- отношения между сущностями и их экземплярами.

Выводы

Таким образом, получены следующие основные результаты:

проведен анализ предметной области, охватывающей порядок создания (эксплуатации) АСЗИ, а также представлено описание модели формирования ТТЗ в части касающейся общих (типовых) требований по защите информации, основанной на положениях как «традиционных», так и относительно новых нормативных документов, изданных по линии «Общих критериев»;

выработан общий алгоритм автоматизированного формирования ТТЗ и сформулированы основные требования к содержанию базы данных системы (элемента системы) поддержки принятия решения заказчика (эксперта).

Представленная модель и выработанный алгоритм позволяют:

сократить время, необходимое заказчику (эксперту) на разработку (рассмотрение, согласование) ТТЗ в части общих (типовых) требований по защите информации;

повысить качество как самого ТТЗ, так и качество создаваемой на его основе АСЗИ.

Дальнейшим направлением повышения качества ТТЗ на создаваемые АСЗИ представляется целесообразным изучение вопросов разработки и использования в рамках системы поддержки принятия решений заказчика (эксперта) соответствующих баз знаний, позволяющих более эффективно формировать специальные (уникальные) требования по защите информации на основе имеющегося опыта и с учетом положений «Общих критериев».

***Рецензент**: Марков Алексей Сергеевич, доктор технических наук, профессор МГТУ им.Н.Э.Баумана, г. Москва, Россия. E-mail: a.markov@bmstu.ru*

Литература

1. Макаренко С.И. Робототехнические комплексы военного назначения - современное состояние и перспективы развития // Системы управления, связи и безопасности. 2016. № 2. С. 73-132.
2. 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.
3. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении. /Под общей редакцией С.Ф.Боева; вводные слова А.И.Смирнова и А.Г.Тормасова; вводная статья И.А.Каляева. -Иннополис: Издательский Дом «Афина», 2017. 440 с.
4. 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.
5. Безденежных С.И. Предложения по совершенствованию порядка проведения опытно-конструкторских работ при создании автоматизированных систем военного назначения // Вооружение и экономика. М., Региональная общественная организация «Академия проблем военной экономики и финансов», 2015. № 1 (30). С. 35-43.

6. 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 международной научно-практической конференции. СПб., Информационный издательский учебно-научный центр «Стратегия будущего», 2013. № 2. С. 71-78.
7. Бакланова Е.Г., Тарадонов С.В. Существенные условия государственного контракта на выполнение научно-исследовательских, опытно-конструкторских и технологических работ для государственных нужд // Вестник МИЭП. 2014. № 3 (16). С.46-55.
8. Бородакий Ю.В., Добродеев А.Ю., Нащекин П.А., Бутусов И.В. О подходах к реализации централизованной системы управлению информационной безопасностью АСУ военного и специального назначения // Вопросы кибербезопасности. 2014. № 2 (3). С. 26-30.
9. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
10. Орлова Ю.А. Алгоритмическое обеспечение анализа текста технического задания и построения моделей программного обеспечения. // Известия Волгоградского государственного технического университета Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах»: межвуз. сб. науч. ст. / ВолгГТУ. Волгоград, 2010. Вып. 8, № 6 (66). С. 68-72.
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. Исаев Г.Н. Проектирование информационных систем: учебное пособие. М., Издательство «Омега-Л», 2013. 424 с.
13. Микони С.В. Теория принятия управленческих решений: учебное пособие. СПб., Издательство «Лань», 2015. 448 с.
14. Бибашов С.А. Предложения по совершенствованию порядка разработки технических заданий на создание автоматизированных систем в защищенном исполнении. В сборнике: Безопасные информационные технологии (БИТ-2017). Сборник трудов Восьмой Всероссийской научно-технической конференции. МГТУ им.Н.Э.Баумана. 2017.

THE MODEL OF FORMATION THE REQUIREMENTS FOR INFORMATION SECURITY TO THE DEVELOPED AUTOMATED SYSTEMS IN THE PROTECTED EXECUTION

***S.Bibashov*[2]**

The article presents the results of the analysis and formal description of the subject area, covering the order of creation of the automated systems in the protected execution and formation of tactical and technical tasks (TTT) on information security issues. A general algorithm for the automated formation of a tactical and technical task and the basic requirements for the structure and content of a database necessary for its software implementation are described. The proposed solutions allow to shorten the time for the development of TTT with the improvement of the quality of the automated system created on its basis.

Keywords: *tactical and technical task, development work, information protection, database, design.*

References

1. Makarenko S.I. Robototekhnicheskie kompleksy voennogo naznacheniya - sovremennoe sostoyanie i perspektivy razvitiya, Sistemy upravleniya, svyazi i bezopasnosti, 2016, N 2, pp. 73-132.
2. Muravnik V.B., Zaharenkov A.I., Dobrodeev A.YU. Nekotorye predlozheniya po podhodu i poryadku realizacii politiki i strategii importozameshcheniya v interesah nacional'noj bezopasnosti i ukrepleniya oboronosposobnosti rossijskoj federacii, Voprosy kiberbezopasnosti, 2016, N 1 (14), pp. 2-8.
3. Petrenko S.A., Stupin D.D. Nacional'naya sistema rannego preduprezhdeniya o komp'yuternom napadenii./Pod obshchej redakciej S.F.Boeva; vvodnye slova A.I.Smirnova i A.G.Tormasova; vvodnaya stat'ya I.A.Kalyaeva. -Innopolis: Izdatel'skij Dom «Afina», 2017. 440 p.

2 Sergey Bibashov, SRTMA. Moscow. E-mail: sbma82@mail.ru

4. CHobanyan V.A., SHahalov I.YU. Analiz i sintez trebovanij k sistemam bezopasnosti ob'ektov kriticheskoj informacionnoj infrastruktury, Voprosy kiberbezopasnosti, 2013, N 1 (1), pp. 17-27.
5. Bezdenezhnyh S.I. Predlozheniya po sovershenstvovaniyu poryadka provedeniya opytno-konstruktorskih rabot pri sozdanii avtomatizirovannyh sistem voennogo naznacheniya, Vooruzhenie i ehkonomika. M., Regional'naya obshchestvennaya organizaciya «Akademiya problem voennoj ehkonomiki i finansov», 2015, N 1 (30), pp. 35-43.
6. Husnulin R.G. Ispol'zovanie tekhnicheskogo zadaniya na zashchitu informacii pri razrabotke integrirovannoj avtomatizirovannoj sistemy upravleniya v zashchishchennom ispolnenii, Fundamental'nye i prikladnye issledovaniya v sovremennom mire. Materialy mezhdunarodnoj nauchno-prakticheskoj konferencii. SPb., Informacionnyj izdatel'skij uchebno-nauchnyj centr «Strategiya budushchego», 2013, N 2, pp. 71-78.
7. Baklanova E.G., Taradonov S.V. Sushchestvennye usloviya gosudarstvennogo kontrakta na vypolnenie nauchno-issledovatel'skih, opytno-konstruktorskih i tekhnologicheskih rabot dlya gosudarstvennyh nuzhd, Vestnik MIEHP, 2014, N 3 (16). P.46-55.
8. Borodakij YU.V., Dobrodeev A.YU., Nashchekin P.A., Butusov I.V. O podhodah k realizacii centralizovannoj sistemy upravleniyu informacionnoj bezopasnost'yu ASU voennogo i special'nogo naznacheniya, Voprosy kiberbezopasnosti, 2014, N 2 (3), pp. 26-30.
9. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody ocenki nesootvetstviya sredstv zashchity informacii. M.: Radio i svyaz', 2012. 192 p.
10. Orlova YU.A. Algoritmicheskoe obespechenie analiza teksta tekhnicheskogo zadaniya i postroeniya modelej programmnogo obespecheniya, Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta Seriya «Aktual'nye problemy upravleniya, vychislitel'noj tekhniki i informatiki v tekhnicheskih sistemah»: mezhvuz. sb. nauch. st. / VolgGTU. Volgograd, 2010. Vyp. 8, № 6 (66), pp. 68-72.
11. Barabanov A.V., Markov A.S., Cirlov V.L. Ocenka sootvetstviya sredstv zashchity informacii «Obshchim kriteriyam», Informacionnye tekhnologii, 2015. V. 21, N 4, pp. 264-270.
12. Isaev G.N. Proektirovanie informacionnyh sistem: uchebnoe posobie. M., Izdatel'stvo «Omega-L», 2013. 424 s.
13. Mikoni S.V. Teoriya prinyatiya upravlencheskih reshenij: uchebnoe posobie. SPb., Izdatel'stvo «Lan'», 2015. 448 p.
14. Bibashov S.A. Predlozheniya po sovershenstvovaniyu poryadka razrabotki tekhnicheskih zadanij na sozdanie avtomatizirovannyh sistem v zashchishchennom ispolnenii. V sbornike: Bezopasnye informacionnye tekhnologii (BIT-2017). Sbornik trudov Vos'moj Vserossijskoj nauchno-tekhnicheskoj konferencii. MGTU im.N.EH.Baumana, 2017.