КОНЦЕПЦИЯ ИТЕРАЦИОННОГО ВНЕШНЕГО ПРОЕКТИРОВАНИЯ ОБЛИКА ПРОАКТИВНЫХ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Горбачев И.Е.[1]

В работе проведен анализ неразрешенных проблем, приводящих к вырождению задач внешнего проектирования (ВНЕПР) систем информационной безопасности (СИБ). Представлена концептуальная схема итерационного системно-агрегативного (ВНЕПР) облика современных СИБ, на основе которой осуществлена формальная постановка задачи обеспечения гарантируемого уровня потенциальной результативности целевого применения проектируемых СИБ, наделенных свойством проактивности. Даны формализованные определения проектного решения (ПрРеш) и облика СИБ. Выявленные на основе данной схемы итерационные связи между этапами жизненного цикла системы (ЖЦС) позволили разработать модель итерационного ВНЕПР облика проактивных СИБ. Особенностью модели являются обоснованные для каждого этапа ЖЦС показатели качества ПрРеш, а также обоснованные цели проведения каждой итерации. Проведенные исследования позволили формально описать специфику функционирования СИБ, наделенных свойством проактивностью, а также сформулировать показатель реализуемости ПрРеш и обосновать показатель готовности системы к непосредственному применению, показатели живучести и функционально-технической (оперативной) готовности.

Ключевые слова: *система информационной безопасности, оценивание эффективности, итерационное внешнее проектирование, проактивность, проектное решение, показатель реализуемости проекта, жизненный цикл системы.*

DOI: 10.21681/2311-3456-2017-5-50-63

Введение

Проблемы, связанные с проектированием и созданием систем информационной безопасности (СИБ), давно находятся в области научного внимания зарубежных и отечественных исследователей, а фундаментальные модели и методы, закладываемые в их основу, базируются на теоретических и прикладных результатах авторитетных научных школ и видных учёных.

Неоценимые результаты получены в области проектирования современных СИБ, рассматриваемой во взаимосвязи с интеллектуальными системами поддержки принятия решений и многоагентными системами (И.В.Котенко) [1, 2], с вопросами анализа и объединения данных для принятия решений и индуктивного обучения (Городецкий В.И., Карсаев О.В.) [3, 4], интеллектуальной обработки данных и извлечения знаний (Городецкий В.И.) [5-7], управления информацией и событиями безопасности (Саенко И.Б.) [8, 9]. Заслуживают особого внимания результаты, связанные с развитием теории динамического управления компьютерной безопасностью (Зегжда П.Д., Зегжда Д.П.) [10, 11].

Однако большинство существующих средств информационной безопасности (ИБ) используют «реактивные» (основанные на реакции системы ИБ на действия злоумышленника) технологии. Данные средства в настоящее время позволяют решать задачи противоборства в критической информационной инфраструктуре (КИИ) лишь в ограниченном объёме и не соответствуют предъявляемым к ним современным требованиям [12].

В значительной степени данное обстоятельство обусловлено отсутствием системного подхода к обоснованию проектных решений (ПрРеш) на создание средств ИБ КИИ и к предъявлению достаточно жестких (современных) требований к образцам создаваемых средств ИБ.

Анализ научно-методического аппарата [13-18], посвященного проблеме обоснования решений при проектировании и реализации систем и средств ИБ КИИ, показывает, что в настоящее время универсальных, формальных методов решения данной задачи не существует. Как правило, данная задача решается экспертно и успех её решения в значительной степени зависит от компетентности и опыта исследователя. По этой причине:

1. Отсутствуют единые методологические подходы и используются различные показатели и

1 Горбачев Игорь Евгеньевич, кандидат технических наук, доцент, Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург, Россия. E-mail: gie1976@mail.ru

критерии оценивания эффективности функционирования СИБ.

2. В технических заданиях смешиваются такие понятия как оперативно-технические требования, технико-экономические показатели, эксплуатационно-технические характеристики и параметры проектируемого изделия ИБ.

3. Разрабатываемые в настоящее время отдельные методики обоснования ПрРеш:

– носят узко-ориентированный характер,

– создаются под заранее определенный облик проектируемого средства и по этой причине непригодны для исследования систем другого облика или построенных на других физических принципах, тем более для СИБ, где противодействие ведётся в виртуальном (нечетком, неопределенном) пространстве.

Представляется совершенно очевидным, что применительно к уникальным, сложным, дорогостоящим системам и процессам противоборства такой путь нереален по следующим причинам:

1) С усложнением СИБ резко возрастает многовариантность технических, проектных, экономических, организационных, управленческих и других решений.

2) Многократно возрастает цена последствий принятия неверного (ошибочного) ПрРеш.

3) Уникальность отдельных СИБ, особенно систем не многократного применения, делает методы исследования их эффективности, основанные на анализе среднего эффекта их применения неприемлемыми. При этом если применяемые в настоящее время методы исследования операций достаточно разработаны и могут считаться приемлемыми для практики, то методы оценивания и анализа эффективности уникальных операций в КИИ изучены мало. Методологические принципы оценивания эффективности уникальных операций в киберпространстве (КП) подробно представлены в трудах [19, 20].

Поиск пригодного научно-методического аппарата оценивания качества СИБ и исследования эффективности их применения в КП наталкивается на существенные трудности, связанные с недостаточной изученностью киберпространства, как среды противоборства [21]. В работе [22] проведен анализ существующих классических кибернетических моделей конфликта применительно к противоборству в КП. Результаты исследований показали, что данные модели имеют существенные недостатки и не приемлемы в исследовании конфликта в киберпространстве. Основной их недостаток заключается в постулирование гипотезы о лежащих на поверхности стратегиях борьбы, в то время как в конфликте данный факт представляет наименьшую ценность – главная задача противоборствующих сторон в киберпространстве – это обнаружить и оценить *скрытые* возможности противника с последующим упреждением его действий.

Это требует совершенствования существующей методологии проектирования проактивных СИБ. Практически реализуемым является лишь способ, основанный на построении достаточно адекватных математических моделей процесса функционирования (ПФ) создаваемых СИБ и сравнения результатов исследования этих моделей. Этот способ является фундаментом внешнего проектирования (ВНЕПР) СИБ, а целью данного проектирования является создание облика Θ этих программно-технических систем, конфликтный характер взаимодействия которых с учетом особенностей противоборства в КП ранее не исследовался

В связи с этим, можно констатировать, что назрела необходимость в создании единого методологического подхода к решению задачи обоснования ПрРеш при ВНЕПР проактивных СИБ в КИИ, основанного на использовании теории эффективности целенаправленных процессов (ТЭЦнП) [23-25]. Основой этой методологии являются комплексный подход к проблеме оценивания качества и вероятностно-гарантированный подход к обеспечению гарантируемого уровня потенциальной результативности применения этих систем.

Фундаментальный вклад в становление и развитие ВНЕПР целеустремленных технических систем (ЦУТС) и целенаправленных процессов функционирования системы (ЦнПФС) как научной дисциплины внесли ученые Петухов Г.Б., Иоффе А.Я., Якунин В.И [24, 25]. Именно они заложили основы методологии исследования эффективности функционирования сложных систем. Однако за рамки их исследований [19] выходило изучение взаимодействия антагонистических систем в информационном конфликте. Анализ ограничений применимости ТЭЦнП для исследования конфликтующих процессов показал, что объект исследования теории ограничен рассмотрением только сплоченных операционных комплексов, а класс разобщенных (антагонистических) ОПК (РОпК) не исследовался.

1. Обоснование непригодности методов внешнего проектирования проактивных систем информационной безопасности

В настоящее время при решении задач ВНЕПР современных СИБ не разрешены следующие проблемы:

1. Качество рассматриваемых систем оценивается по отдельным параметрам, что позволяет анализировать лишь отдельные стороны информационного конфликта вне рамок системного подхода.

2. В большинстве случаев (и это в лучшем случае) под показателем качества СИБ понимается вектор, включающий несколько независимых показателей свойств системы или показатель, характеризующий лишь одно из существенных свойств системы. При этом не учитывается, что показатель качества – это комплексное понятие, а не простое множество взаимно независимых показателей свойств объекта, поскольку между отдельными свойствами объекта могут существовать связи, которые в терминах теории множеств не описываются.

3. Зачастую эффективным считается такое функционирование СИБ, при котором она технически (технологически) способна выполнить определенную (частную) задачу при определенных (детерминированных) условиях. При этом не учитывается ни случайный характер объема и степени (уровня) обработки данных, ни случайный характер воздействия нарушителя, ни нечеткий характер среды информационного конфликта.

4. При оценивании эффективности процесса функционирования средств информационной безопасности (ИБ) не учитывается взаимосвязь и зависимость компонент $V_{\langle n_1 \rangle}$, $R_{\langle n_2 \rangle}$, $T_{\langle n_3 \rangle}$ вектора показателя $U_{\langle n \rangle}$ качества результатов операции, проводимой СИБ (например, зависимость между величиной предотвращенного ущерба, затратами ресурсов и операционного времени на противодействие нарушителю). Компоненты $V_{\langle n_1 \rangle}$, $R_{\langle n_2 \rangle}$, $T_{\langle n_3 \rangle}$ характеризуют соответственно результативность операции, ресурсоемкость операции и оперативность операции.

5. В отдельных случаях оценивание качества процесса функционирования средств ИБ производится без предъявления требований к результатам операции.

6. В большинстве случаев не строится математическая модель кибернарушителя, не исследуется характер его возможных действий, не определяются характеристики $B''_{\langle l'' \rangle}$ формируемой нарушителем операционной ситуации, не исследуются возможные пути скрытого рефлексивного управления его поведением и изменения его потенциальных возможностей [21, 22]. Обычно противник «агрегируется» в виде некоторых требований $U^{\partial}_{\langle 3 \rangle}\left(B''_{\langle l'' \rangle} \right)$ к результатам $U_{\langle 3 \rangle}$ операции, например, суперсистемой априори задаются директивные требования ко времени окончания проведения нарушителем операции. Иными словами, нарушитель моделируется посредством задания детерминированных требований. Не исследуется нарушитель как человеко-машинная система, наделенная «интеллектом», «разумом», что характерно для киберпространства [22].

7. Уделено недостаточно внимания методологическим аспектам проблемы построения математических моделей таких сложных объектов как КИИ и кибернарушитель. Точнее сказать, мало обсуждаются принципы и методики их построения и основные требования, которым они должны удовлетворять. В основном говорится, что такое математические модели, и приводятся их примеры и не говорится о том, как эти модели построить и какими они должны быть, чтобы их можно было использовать в конкретных прикладных исследованиях, то есть не исследуется качество этих моделей применительно к решаемой задаче. Мало говорится о специфике моделей объектов КИИ и моделей нарушителя в исследовании ИБ вообще и в рамках задачи исследования эффективности организации защиты в частности.

Перечисленные проблемы являются принципиальными и их игнорирование приводит к вырождению задачи ВНЕПР СИБ. По этой причине существующая методология проектирования СИБ не позволяет оценить и обеспечить гарантируемый уровень потенциальной результативности целевого применения проектируемых СИБ, наделенных свойством проактивности.

В результате, основным ограничением методов ВНЕПР СИБ является их *неприменимость* для исследования так называемых РОпК, в состав которых входят антагонистические системы – «система ИБ – кибернарушитель». Универсальных формальных методов ВНЕПР таких систем с прогнозируемым эффектом их поведения в настоящее время не существует [19, 25]. Следствием вышесказанного является отсутствие на этапе ВНЕПР методов обоснования проектных решений (ПрРеш) при разработке проактивных СИБ. В связи с этим в работах [19, 26] была обоснована типовая структура РОпК моделирования противоборства в КИИ.

Очевидно, что в условиях ограничений на выделенные ресурсы не всегда возможно создать проактивную СИБ требуемого качества. *Для разрешения этого конфликта* необходимо реализовать *итерационный подход*, то есть реализовать обратные связи между этапами и подэтапами жизненного цикла системы (ЖЦС) СИБ, что в настоящее время при проектировании данных проактивных систем не выполняется.

Таким образом, можно сделать вывод, что проблема итерационного системно-агрегативного ВНЕПР облика Θ проактивных СИБ до настоящего времени не нашли должного отражения в исследованиях. Как следствие, научно-техническая проблема обеспечения обоснованности принятия ПрРеш при разработке проактивных СИБ в КИИ в настоящее время является весьма актуальной.

Цель проведения исследований состоит в обосновании показателя Π качества проектных решений для каждого этапа ЖЦС при итерационном ВНЕПР СИБ.

2. Концептуальная схема итерационного системно-агрегативного (внешнего) проектирования облика проактивных систем информационной безопасности

Этапы ЖЦС СИБ представляют собой процесс, в котором условия (характеристики КИИ) $B'_{\langle l' \rangle}$ функционирования СИБ и условия (характеристики нарушителя) $B''_{\langle l'' \rangle}$ ее целевого применения являются исходными для этапа обоснования облика Θ системы. Проведенный анализ специфики задач, решаемых в ходе проектирования СИБ, позволил разработать концептуальную схему итерационного системно-агрегативного ВНЕПР облика проактивных СИБ (рис. 1).

Определение 1. Облик Θ СИБ есть область $\left\{ A'^{\,\partial}_{\langle k' \rangle} \right\}$ допустимых значений агрегатов $A'_{\langle k' \rangle}$ (агрегированных характеристик) системы, полученных на этапе ее ВНЕПР и обеспечивающих гарантируемый уровень $v^{\Gamma}_{ПР}$ превосходства в конфликте:

$$v^{\Gamma}_{ПР} = f^{-1}(P^{\Gamma}_{ДЦ}(\gamma;\Theta),\tau^{Д},\gamma), \qquad (1)$$

где $v^{\Gamma}_{ПР}$ – гарантируемый уровень потенциальной результативности v целевого примене-

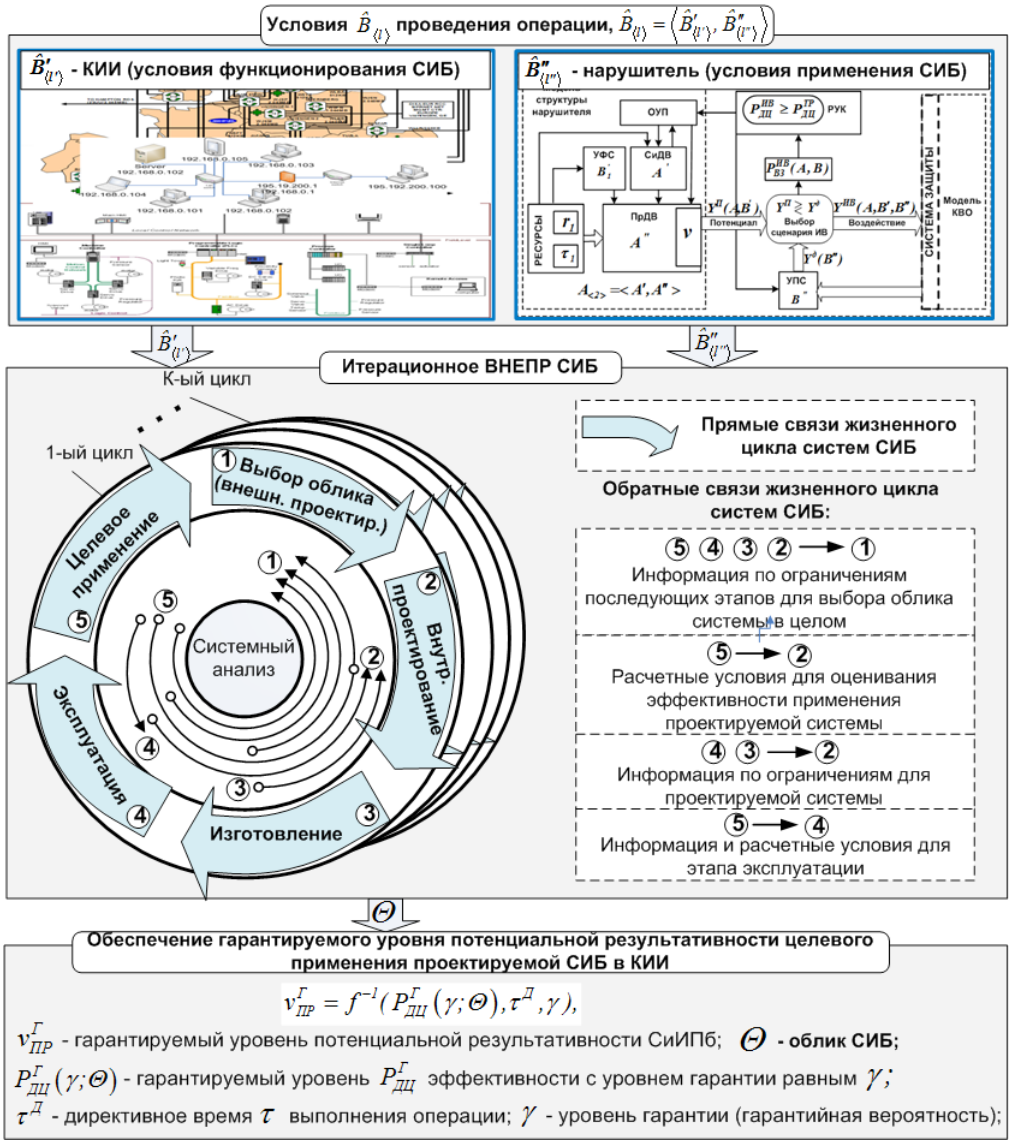

Рис. 1. *Концептуальная схема итерационного системно-агрегативного ВНЕПР облика проактивных СИБ*

ния проектируемых СИБ (гарантируемый уровень потенциального целевого эффекта); $P^{\Gamma}_{ДЦ}\left(\gamma; A'^{ПР}_{\langle k'\rangle}\right)$ – гарантируемый уровень превосходства в конфликте с уровнем гарантии равным γ; γ – уровень гарантии (гарантийная вероятность); $\tau^{Д}$ – директивное (максимально допустимое) время τ выполнения операции.

Замечание 1. В широком смысле облик СИБ определяется как задачами, для которых она предназначена, так и типом, числом средств, включаемых в состав системы, и их параметрами.

Определение 2. Проектное решение на этапе ВНЕПР есть совокупность значений агрегатов $A'^{\partial}_{\langle k'\rangle}$ (агрегированных характеристик), специфицирующих облик Θ проектируемой СИБ и обеспечивающих гарантируемый уровень $v^{\Gamma}_{ПР}$ потенциальной результативности целевого применения этих систем в информационном конфликте.

По физическому смыслу $P^{\Gamma}_{ДЦ}\left(\gamma;\Theta\right)$ есть гарантируемая (минимально возможная) вероятность достижения цели операции с уровнем гарантии равным γ (при условии, что к результатам операции предъявлены требования $\left\langle v^{T}, \tau^{Д}\right\rangle$), где v^{T} – требуемая потенциальная результативность целевого применения СИБ.

В качестве рациональных ПрРеш выбираются наиболее «экономичные» $A'^{ЭК}_{\langle k'\rangle}$ по критерию пригодности значения характеристик $A'^{\partial}_{\langle k'\rangle}$, $A'^{ЭК}_{\langle k'\rangle} \in \left\{ A'^{\partial}_{\langle k'\rangle} \right\}$

Для каждого этапа ЖЦС формализуем особенности и цели проведения итерационного ВНЕПР СИБ в КИИ.

3. ЭТАП 1. Формализация задачи обоснования проектного решения на этапе внешнего проектирования облика проактивных систем информационной безопасности

При обосновании облика Θ СИБ на этапе ВНЕПР определяется тип каждой ее подсистемы на основе анализа целей, поставленных перед системой, и ее основных характеристик. Объектом исследования является процесс функционирования системы в целом; каждая подсистема задается основными (обликовыми, агрегированными) параметрами (агрегатами), определяющими ее роль и место в информационном конфликте. На этом этапе определяется перечень задач, которые должна решать система, способы достижения основных целей, а также роль и место этой системы в системе более высокого уровня (суперсистеме). При этом определяются критерии оценивания, исследуется эффективность применения, стоимость и сроки создания и функционирования рассматриваемых вариантов построения системы, а также оценивается степень риска создания системы по выбранным показателям. Результат достигается при итеративном процессе исследований.

Показатель $П_1$ качества ПрРеш на первом этапе может быть представлен в виде

$$П_1 = f\left(A_{\langle k\rangle}, B_{\langle l\rangle}, T_1, C_1; I\left({}_2A^{пп}_{\langle k\rangle}\right), I\left({}_5B^{прим}_{\langle l\rangle}\right)\right), \quad (2)$$

где $П_1$ – показатель качества ПрРеш на первом этапе, учитывающий стоимость C_1 работ по проведению ВНЕПР и обоснованию требуемого уровня $P^{ТР}_{ДЦ}$ показателя $P_{ДЦ}$ эффективности ЦнПФС при директивных затратах $T^{Д}_1$ времени T_1, $T_1 = T\left({}_2A^{пп}_{\langle k\rangle}\right)$, $C_1 = C\left({}_2A^{пп}_{\langle k\rangle}\right)$; $A_{\langle k\rangle}$ – рассматриваемые на первом этапе значения вектора $A'_{\langle k'\rangle}$ характеристик СИБ и вектора $A''_{\langle k''\rangle}$ характеристик организации (технологии) ее применения, $A_{\langle k\rangle} = \left\langle A'_{\langle k'\rangle}, A''_{\langle k''\rangle}\right\rangle$, $k = k' + k''$; $\mathrm{B}_{\langle l\rangle}$ – рассматриваемые на первом этапе значения вектора $B'_{\langle l'\rangle}$ характеристик условий функционирования и вектора $\mathrm{B}''_{\langle l''\rangle}$ характеристик условий применения проектируемой СИБ, $B_{\langle l\rangle} = \left\langle B'_{\langle l'\rangle}, B''_{\langle l''\rangle}\right\rangle$, $B_{\langle l\rangle} = B_{\langle l\rangle}\left({}_5B^{прим}_{\langle l\rangle}\right)$, $l = l' + l''$; $I\left({}_2A^{пп}_{\langle k\rangle}\right)$ – полученные со второго этапа данные о конкретных значениях параметров (проектных параметров) $A'^{пп}_{\langle k'\rangle}$ проектируемой СИБ и конкретных значениях характеристик $A''^{пп}_{\langle k''\rangle}$ технологии ее применения; $I\left({}_5B^{прим}_{\langle l\rangle}\right)$ – полученные с пятого этапа данные о реальных значениях характеристик $B'^{(прим)}_i$ условий функционирования проектируемой СИБ (т. е. характеристик защищаемого объекта КИИ) и реальных значениях характеристик $B''^{(прим)}_i$ условий ее применения (т. е. характеристик нарушителя).

Показатель (2) можно представить в виде

$$П_1 = \varphi\left(P_Ц, T_1, C_1; I\left({}_2A^{пп}_{\langle k\rangle}\right), I\left({}_5B^{прим}_{\langle l\rangle}\right)\right), \quad (3)$$

где $P_Ц$ – условная вероятность [25] выполнения задачи СИБ.

Наибольший практический интерес представляет априорная оценка качества ПрРеш для проектируемых систем, то есть еще до их применения. Поэтому для управления качеством СИБ ее необходимо оценивать в процессе изготовления и даже еще раньше – на этапе разработки ПрРеш.

Таким образом, *прогноз качества СИБ* необходим на этапах её проектирования и выработки ПрРеш, а *оценка качества* – на этапе изготовления и приемных испытаний, предшествующем ее применению в реальных условиях.

На этапе ВНЕПР априорное оценивание качества СИБ без прямого ее применения по назначению возможно, если известно соотношение, связывающее ее характеристики (структуру, организацию, параметры, ЭТХ и т.п.) с выходным эффектом $U_{\langle n\rangle}$ ее целевого применения [19, 26]:

$$U_{\langle n\rangle}\left(A_{\langle k\rangle};B'_{\langle l'\rangle}\right)=U_{\langle n\rangle}\left(A'_{\langle k'\rangle};A''_{\langle k''\rangle},B'_{\langle l'\rangle}\right), \quad (4)$$

где $A'_{\langle k'\rangle}$ – эксплуатационно-технические характеристики (ЭТХ) СИБ; $A''_{\langle k''\rangle}$ – параметры организации целенаправленного процесса функционирования СИБ; $B'_{\langle l'\rangle}$ – характеристики условий функционирования СИБ (характеристики КИИ); $A_{\langle k\rangle}=<A'_{\langle k'\rangle},A''_{\langle k''\rangle}>$, $B_{\langle l\rangle}=<B'_{\langle l'\rangle},B''_{\langle l''\rangle}>$.

Тогда, если для оператора (4) существует обратный оператор по вектору $A'_{\langle k'\rangle}$:

$$A'_{\langle k'\rangle}=A'_{\langle k'\rangle}\left(U_{\langle n\rangle};A''_{\langle k''\rangle},B'_{\langle l'\rangle}\right)=U^{-1}_{\langle k'\rangle}\left(U_{\langle n\rangle};A''_{\langle k''\rangle},B'_{\langle l'\rangle}\right), \quad (5)$$

позволяющий выразить зависимость возможных значений $A'_{\langle k'\rangle}$ агрегированных характеристик СИБ от выходных эффектов $U_{\langle n\rangle}$, параметров $A''_{\langle k''\rangle}$ организации ЦнПФС и характеристик $B'_{\langle l'\rangle}$ условий функционирования системы, то может быть определена область $\left\{A'^{\,\partial}_{\langle k'\rangle}\right\}$ допустимых значений $A'^{\,\partial}_{\langle k'\rangle}$ вектора $A'_{\langle k'\rangle}$ параметров и ЭТХ СИБ, при которых она способна выполнить свои функции, соответствующая области $\left\{U^{\partial}_{\langle n\rangle}\right\}$ допустимых значений $U^{\partial}_{\langle n\rangle}$ результатов $U_{\langle n\rangle}$ ЦнПФС, то есть

$$\left\{U^{\partial}_{\langle n\rangle}\right\}\Rightarrow\left\{A'^{\,\partial}_{\langle k'\rangle}\right\}=\left\{A'^{\,\partial}_{\langle k'\rangle}:U_{\langle n\rangle}\left(A'^{\,\partial}_{\langle k'\rangle};A''^{\,H}_{\langle k''\rangle},B'^{\,H}_{\langle l'\rangle}\right)\in\right.$$
$$\left.\in\left\{U^{\partial}_{\langle n\rangle}\left(B''^{\,H}_{\langle l''\rangle}\right)\right\}\right., \quad (6)$$

где за знаком «;» перечисляются не переменные, а параметры функции, то есть постоянные величины; $A''^{\,H}_{\langle k''\rangle}$ – номинальные (расчетные) значения характеристик организации ЦнПФС; $B'^{\,H}_{\langle l'\rangle}$ – номинальные (расчетные) значения характеристик условий $B'_{\langle l'\rangle}$ функционирования СИБ; $B''^{\,H}_{\langle l''\rangle}$ – номинальные (расчетные) значения характеристик условий $B''_{\langle l''\rangle}$ применения СИБ (номинальные (расчетные) значения характеристик противника).

Замечание 1. Выражение (6) определяет *формализованную постановку задачи обоснования ПрРеш* на этапе ВНЕПР.

Утверждение 1. Область $\left\{A'^{\,\partial}_{\langle k'\rangle}\right\}$ физически характеризует множество *допустимых* вариантов ПрРеш $A'^{\,\partial}_{\langle k'\rangle}$, специфицирующих облик Θ проектируемой системы ИПб на этапе ВНЕПР, то есть $\Theta=\left\{A'^{\,\partial}_{\langle k'\rangle}\right\}$.

Следствие 1. Значение вектора $A'^{\,\partial}_{\langle k'\rangle}$ на этапе ВНЕПР определяет конкретное пригодное ПрРеш, удовлетворяющее критерию пригодности по эффективности $G_{Э}: P_{ДЦ}\left(A'^{\,\partial}_{\langle k'\rangle}\right)\geq P^{TP}_{ДЦ}$, но не обеспечивающее гарантируемый уровень $P^{Г}_{ДЦ}\left(\gamma;A'^{\,ЭК}_{\langle k'\rangle}\right)$ (рис.1) эффективности применения проектируемой СИБ с уровнем гарантии γ, где $P_{ДЦ}$ – показатель эффективности функционирования СИБ, $P^{TP}_{ДЦ}$ – требуемое значение вероятности $P_{ДЦ}$ достижения цели информационной операции.

Замечание 2. Результатами ВНЕПР СИБ являются:

– значения ЭТХ $A'_{\langle k'\rangle}$ (агрегаты) облика проектируемой СИБ;

– значения параметров $A''_{\langle k''\rangle}$ (агрегаты) организации ЦнПФС;

– значение показателя C_1 стоимости разработки ПрРеш;

– предельная стоимость и директивные сроки проведения ВНУПР $(C^{П}_2,T^{Д}_2)$, создания $(C^{П}_3,T^{Д}_3)$, эксплуатации $(C^{П}_4,T^{Д}_4)$ и целевого применения $(C^{П}_5,T^{Д}_5)$ рассматриваемых вариантов ПрРеш.

Замечание 3. Руководствуясь методом главной компоненты [25] ПрРеш считается обоснованным на этапе ВНЕПР, если показатель C_1 достигает требуемого уровня, а остальные показатели T_1 и $P_{Ц}$ удовлетворяют некоторой системе ограничений, то есть реализуется следующий критерий G_1 пригодности:

$$G_1:\begin{cases}C_1\leq C^{П}_1;\\ P_{Ц}\geq P^{TP}_{Ц},\ T_1\leq T^{Д}_1,\end{cases} \quad (7)$$

где $C^{П}_1$ – предельная стоимость C_1 проведения ВНЕПР СИБ (выработки ПрРеш).

4. ЭТАП 2. Формализация задачи обоснования проектного задания на этапе внутреннего проектирования проактивных систем информационной безопасности

На этапе ВНУПР определяются конкретные значения проектных ЭТХ $A'^{\,пп}_{\langle k'\rangle}$ проектируемой системы и значения проектных параметров $A''^{\,пп}_{\langle k''\rangle}$ организации ее целевого применения, вырабатывается ПрЗад на изготовление СИБ и организацию ее ПФ. Учитываются следующие данные, полученные на первом этапе:

– значения агрегированных характеристик $A'_{\langle k'\rangle}$ СИБ и характеристик $A''_{\langle k''\rangle}$ организации ее применения;

– облик Θ проектируемой системы, то есть область $\left\{A'^{\,\partial}_{\langle k'\rangle}\right\}$ допустимых значений агрегатов (обликовых параметров);

– область возможных значений параметров $B'_{\langle l'\rangle}$ модели условий функционирования и параметров $B''_{\langle l''\rangle}$ условий применения СИБ;

– РОпК применения СИБ в КИИ [19, 26];

– критерий $G_{ЦР}$ оценивания качества возможных результатов операции [19];

– критерии $G_{ЦЭ}$ и $O_{ЦЭ}$ оценивания эффективности применения СИБ [26];

– варианты ПрРеш $A'^{\partial}_{\langle k'\rangle}$ в условиях выполнения критерия (6) и ограничений, сформулированных на первом этапе.

Далее обосновываются рациональные варианты $\left\{A'^{p(nn)}_{\langle k'\rangle}\right\}$ проектируемых СИБ в условиях выполнения значений обликовых (агрегированных) параметров $\left\{A'^{\partial}_{\langle k'\rangle}\right\}$ и ограничений, сформулированных на первом этапе.

Качество вариантов проектируемых СИБ определяется:

– моделированием этапа непосредственного применения в условиях воздействия нарушителя при учете основных особенностей и ограничений третьего и четвертого этапов;

– качеством имеющейся производственной базы;

– условиями изготовления и эксплуатации.

Показатель $П_2$ качества ПрРеш на этом этапе может быть представлен как

$$П_2 = f\left({}_2A^{nn}_{\langle k\rangle}, {}_2B^{nn}_{\langle l\rangle}, T_2, C_2; I\left({}_3A^{изг}_{\langle k'\rangle}\right), I\left({}_5B^{прим}_{\langle l\rangle}\right)\right) = \\ = \varphi\left(P_Ц, T_2, C_2; I\left({}_3A^{изг}_{\langle k'\rangle}\right), I\left({}_5B^{прим}_{\langle l\rangle}\right)\right), \quad (8)$$

где $П_2$ – показатель качества ПрРеш на втором этапе, учитывающий затраты C_2 для обеспечения требуемого уровня $P^{ТР}_Ц$ показателя $P_Ц$ условной вероятности выполнения задачи при директивных затратах $T^{Д}_2$ времени T_2, $T_2 = T\left({}_2A^{nn}_{\langle k\rangle}\right)$ $C_2 = C\left({}_2A^{nn}_{\langle k\rangle}\right)$; $B^{nn}_{\langle l\rangle} = B^{nn}_{\langle l\rangle}\left({}_5B^{прим}_{\langle l\rangle}\right)$; $I\left({}_3A^{изг}_{\langle k'\rangle}\right)$ – полученная по результатам третьего этапа информация о характеристиках $A'^{изг}_{\langle k'\rangle}$ проектируемой СИБ и характеристиках $A''^{изг}_{\langle k''\rangle}$ технологии ее применения.

Формальная постановка задачи обоснования ПрЗад на этапе ВНУПР имеет следующее выражение:

$$A'^{p(nn)}_{\langle k'\rangle} = \underset{A'_{\langle k'\rangle}\in\left\{A'^{\partial}_{\langle k'\rangle}\right\}}{arg}\left\{C_2\left(A'^{nn}_{\langle k'\rangle}(A'^{\partial}_{\langle k'\rangle})\right) \le C^{П}_2 \,/\right. \\ \left./\left(P_Ц\left(A'^{nn}_{\langle k'\rangle}(A'^{\partial}_{\langle k'\rangle})\right) \ge P^{ТР}_Ц\right) \cap \left(T_2\left(A'^{nn}_{\langle k'\rangle}(A'^{\partial}_{\langle k'\rangle})\right) \le T^{Д}_2\right)\right\} \quad (9)$$

или

$$A'^{p(nn)}_{\langle k'\rangle} = \underset{A'_{\langle k'\rangle}\in\left\{A'^{\partial}_{\langle k'\rangle}\right\}}{arg}\left\{T_2\left(A'^{nn}_{\langle k'\rangle}(A'^{\partial}_{\langle k'\rangle})\right) \le T^{Д}_2 \,/\right. \\ \left./\left(P_Ц\left(A'^{nn}_{\langle k'\rangle}(A'^{\partial}_{\langle k'\rangle})\right) \ge P^{ТР}_Ц\right) \cap \left(C_2\left(A'^{nn}_{\langle k'\rangle}(A'^{\partial}_{\langle k'\rangle})\right) \le C^{П}_2\right)\right\}, \quad (10)$$

где $A'^{p(nn)}_{\langle k'\rangle}$ – допустимое ПрЗад $A'^{nn}_{\langle k'\rangle}$ из области $\left\{A'^{p(nn)}_{\langle k'\rangle}\right\}$ допустимых значений характеристик проектируемой СИБ; $C^{П}_2$ – обоснованная на этапе ВНЕПР предельная стоимость C_2 проведения ВНУПР СИБ (выработки ПрЗад); $T^{Д}_2$ – обоснованные на этапе ВНЕПР директивные затраты времени T_2 на выработку ПрЗад.

Замечание 4. Область $\left\{A'^{p(nn)}_{\langle k'\rangle}\right\}$ на этапе ВНУПР характеризует множество рациональных вариантов ПрЗад на изготовление СИБ, соответственно, конкретное значение вектора $A^{p(nn)}_{\langle k'\rangle}$ определяет конкретное допустимое ПрЗад на изготовление СИБ.

Замечание 5. Область $\left\{A'^{p(nn)}_{\langle k'\rangle}\right\}$ фактически определяет для третьего этапа область рациональных значений проектных параметров и характеристик проектируемой СИБ.

Замечание 6. Результатами этапа ВНУПР являются:

– $\left\{A'^{p(nn)}_{\langle k'\rangle}\right\}$ – множество допустимых вариантов ПрЗад на изготовление СИБ;

– $\left\{\Delta^{экс}_{\langle n\rangle}\left(A''^{(nn)}_{\langle k''\rangle}\right)\right\}$ – множество возможных алгоритмов эксплуатации СИБ (на этапе целевого применения);

– $\left\{\Lambda^{прим}_{\langle m\rangle}\left(A''^{(прим)}_{\langle k''\rangle}\right)\right\}$ – множество возможных сценариев применения СИБ.

5. ЭТАП 3. Формализация задачи обоснования технологического решения на этапе изготовления проактивных систем информационной безопасности

На третьем этапе изготавливается СИБ в соответствии с требованиями конструкторской документации, разработанной в соответствии с ПрЗад второго этапа (этапа ВНУПР), при выделенных материальных и временных затратах $C^{П}_3$ и $T^{Д}_3$, соответственно, на конкретной производственной базе. В качестве ведущих рассматриваются показатели стоимости $C_3 = C\left({}_3A_{\{k\}}, П^{ТП}_3\right)$ и срока $T_3 = T\left({}_3A_{\{k\}}, П^{ТП}_3\right)$ изготовления элементов СИБ, где $П^{ТП}_3$ – показатель качества технологического процесса изготовления на третьем этапе. Анализ показателей C_3 и T_3 обуславливает решение по совершенствованию качества технологического процесса.

Учет взаимосвязи проектно-конструкторских и технологических решений предусматривается на этапе проектирования, когда особенности технологического процесса учитываются при принятии ПрЗад $A^{p(nn)}_{\langle k'\rangle}$ как обратная связь третьего и второго этапов. Поэтому анализ качества ПрЗад на этапе

изготовления системы может быть направлен на принятие решения на коррекцию качества проведения ВНУПР в случае выхода параметров $A^{изг}_{\langle k'\rangle}$ из области $\left\{A'^{p(пп)}_{\langle k'\rangle}\right\}$ в процессе изготовления.

Показатель $П_3$ качества ПрРеш на этом этапе может быть представлен как

$$П_3 = f\left({}_3A'^{изг}_{\langle k'\rangle}, {}_2B^{пп}_{\langle l\rangle}, T_3, C_3\right) = П_3\left(P_Ц, T_3, C_3\right), \quad (11)$$

где $П_3$ – показатель качества ПрРеш на четвертом этапе, отражающий возможность обеспечения требуемого уровня $P^{ТР}_Ц$ показателя $P_Ц$ условной вероятности выполнения задачи при заданных на этапе ВНЕПР предельных затратах $C^{П}_3$ ресурсов C_3 и заданных директивных затратах $T^{Д}_3$ времени T_3 на изготовление СИБ, $T_3 = T\left({}_3A'^{изг}_{\langle k'\rangle}, П^{ТП}_3\right)$, $C_3 = C\left({}_3A'^{изг}_{\langle k'\rangle}, П^{ТП}_3\right)$; $П^{ТП}_3$; – показатель качества технологического процесса изготовления СИБ; ${}_2B^{пп}_{\langle l\rangle}$ – значения параметров ${}_3B^{изг}_{\langle l\rangle}$ условий проведения операции определяются обоснованными на втором этапе значениями параметров ${}_2B^{пп}_{\langle l\rangle}$ условий проведения операции, ${}_3B^{изг}_{\langle l\rangle} = {}_2B^{пп}_{\langle l\rangle}$.

Формальная постановка задачи обоснования технологического решения (ТехнРеш) на третьем этапе имеет следующее выражение:

$$A'^{p(изг)}_{\langle k'\rangle} = \underset{A'_{\langle k'\rangle}\in\left\{A'^{д}_{\langle k'\rangle}\right\}}{arg}\left\{C_3\left(A'^{изг}_{\langle k'\rangle}\left(A'^{p(пп)}_{\langle k'\rangle}\right)\right)\le C^{П}_3 \;/\right.$$

$$\left./\left(P_Ц\left(A'^{изг}_{\langle k'\rangle}\left(A'^{p(пп)}_{\langle k'\rangle}\right)\right)\ge P^{ТР}_Ц\right)\cap\left(T_3\left(A'^{изг}_{\langle k'\rangle}\left(A'^{p(пп)}_{\langle k'\rangle}\right)\right)\le T^{Д}_3\right)\right\}, \quad (12)$$

где $A'^{p(изг)}_{\langle k'\rangle}$ – рациональное ТехнРеш $A'^{(изг)}_{\langle k'\rangle}$ из области $\left\{A'^{p(изг)}_{\langle k'\rangle}\right\}$ рациональных значений, пригодных для технологического изготовления;

Замечание 7. Результатами реализации третьего этапа являются:

– изготовленная СИБ с ЭТХ $A'^{p(изг)}_{\langle k'\rangle}$;

– определяемые в ходе приемных испытаний номинальные (расчетные) значения $A''^{H}_{\langle k''\rangle}$ и $B'^{H}_{\langle l'\rangle}$ для этапа ВНЕПР;

– $B''^{H}_{\langle l''\rangle}$ – определяемые в ходе приемных испытаний номинальные (расчетные) значения характеристик $B''_{\langle l''\rangle}$;

– определяемые в ходе приемных испытаний допустимые значения $A'^{д}_{\langle k'\rangle}$ параметров $A'_{\langle k'\rangle}$.

6. ЭТАП 4. Формализация задачи обоснования рационального алгоритма эксплуатации проактивных систем информационной безопасности

На четвертом этапе реализуются алгоритмы $\Delta^{экс}_{\langle n\rangle}$ эксплуатации и технического обслуживания СИБ (например, периодичность обновления базы сигнатур компьютерных вирусов), разработанные на этапе их проектирования. Анализ качества ПрРеш на этом этапе направлен на разработку рациональных алгоритмов $\Delta^{p(экс)}_{\langle n\rangle}$ эксплуатации системы на основе обработки оперативной информации, получаемой, например, средствами SIEM-систем.

Показатель $П_4$ качества ПрРеш на этом этапе может быть представлен как

$$П_4 = f\left({}_4A''^{экс}_{\langle k''\rangle}, {}_4B^{экс}_{\langle l\rangle}, T_4, C_4; I\left({}_4A''^{экс}_{\langle k''\rangle}\right), I\left({}_5B^{прим}_{\langle l\rangle}\right)\right) =$$
$$= \varphi\left(P_Ц, T_4, C_4; I\left({}_4A''^{экс}_{\langle k''\rangle}\right), I\left({}_5B^{прим}_{\langle l\rangle}\right)\right), \quad (13)$$

где $П_4$ – показатель качества ПрРеш на четвертом этапе, учитывающий возможность обеспечения требуемого уровня $P^{ТР}_Ц$ показателя $P_Ц$ условной вероятности выполнения задачи при заданных на этапе ВНЕПР предельных затратах $C^{П}_4$ ресурсов C_4 и заданных директивных затратах $T^{Д}_4$ времени T_4; $B^{экс}_{\langle l\rangle} = B^{экс}_{\langle l\rangle}\left({}_5B^{прим}_{\langle l\rangle}\right)$; $I\left({}_4A''^{экс}_{\langle k''\rangle}\right)$ – актуализированная на четвертом этапе информация о характеристиках $A''^{экс}_{\langle k''\rangle}$ технологии применения СИБ.

Математическая формулировка задачи обоснования рационального алгоритма $\Delta^{p(экс)}_{\langle n\rangle}$ эксплуатации СИБ на четвертом этапе имеет следующее выражение:

$$\Delta^{p(экс)}_{\langle n\rangle} = \underset{\Delta^{экс}_{\langle n\rangle}\in\left\{\Delta^{д}_{\langle n\rangle}\right\}}{arg}\left\{P_Ц\left(\Delta^{экс}_{\langle n\rangle}\left(A'^{p(изг)}_{\langle k'\rangle}\right); A''^{экс}_{\langle k''\rangle}\right)\ge P^{ТР}_Ц \;/\right.$$

$$/\left(C_4\left(\Delta^{экс}_{\langle n\rangle}\left(A'^{p(изг)}_{\langle k'\rangle}\right); A''^{экс}_{\langle k''\rangle}\right)\le C^{П}_4\right)\cap$$

$$\left.\cap\left(T_4\left(\Delta^{экс}_{\langle n\rangle}\left(A'^{p(изг)}_{\langle k'\rangle}\right); A''^{экс}_{\langle k''\rangle}\right)\le T^{Д}_4\right)\right\}, \quad (14)$$

где $\Delta^{p(экс)}_{\langle n\rangle}$ –допустимый алгоритм эксплуатации СИБ (характеризуемой параметрами $A'^{p(изг)}_{\langle k'\rangle}$), полученный на основе обработки оперативной информации $I\left({}_4A''^{экс}_{\langle k''\rangle}\right)$, $I\left({}_5B^{прим}_{\langle l\rangle}\right)$, добытой средствами «рефлексии» на четвертом этапе.

7. ЭТАП 5. Формализация задачи обоснования рационального сценария целевого применения проактивных систем информационной безопасности

На этапе организации целевого применения СИБ и управления операцией определяются сценарии наилучшего использования системы в конкретной среде КИИ с учетом специфики целевой обстановки, опыта использования подобных систем, искусства лица, принимающего решение.

На этом этапе реализуются сценарии $\Lambda^{прим}_{\langle m\rangle}$ непосредственного целевого применения СИБ, разработанные на этапе их проектирования. Анализ качества ПрРеш направлен на разработку раци-

ональных сценариев $\Lambda_{\langle n\rangle}^{p(прим)}$ применения системы с учетом имеющейся информации об условиях ${}_5B_{\langle l\rangle}^{прим}$ проведения информационной операции, ${}_5B_{\langle l\rangle}^{прим} = \left\langle {}_5B_{\langle l'\rangle}^{\prime прим}, {}_5B_{\langle l''\rangle}^{\prime\prime прим} \right\rangle$: ${}_5B_{\langle l'\rangle}^{\prime прим}$ – параметры условий функционирования СИБ; ${}_5B_{\langle l''\rangle}^{\prime\prime прим}$ – характеристики противника (параметры условий применения СИБ).

Показатель $П_5$ качества ПрРеш на этом этапе может быть представлен как

$$П_5 = f\left({}_5A_{\langle k''\rangle}^{\prime\prime прим}, {}_5B_{\langle l\rangle}^{прим}, T_5, C_5, I\left({}_5A_{\langle k''\rangle}^{\prime\prime прим}\right), I\left({}_5B_{\langle l\rangle}^{прим}\right)\right) =$$

$$= \varphi\left(P_Ц, T_5, C_5, I\left({}_5A_{\langle k''\rangle}^{\prime\prime прим}\right), I\left({}_5B_{\langle l\rangle}^{прим}\right)\right), \quad (15)$$

где $П_5$ – показатель качества ПрРеш на пятом этапе, отражающий возможность обеспечения требуемого уровня $P_Ц^{ТР}$ показателя $P_Ц$ условной вероятности выполнения задачи при заданных на этапе ВНЕПР предельных затратах $C_5^{П}$ ресурсов C_5 и заданных директивных затратах $T_5^{Д}$ времени T_5; $I\left({}_5A_{\langle k''\rangle}^{\prime\prime прим}\right)$ – актуализированные на пятом этапе данные о характеристиках $A_{\langle k''\rangle}^{\prime\prime прим}$ технологии применения СИБ; $I\left({}_5B_{\{l\}}^{прим}\right)$ – актуализированные на пятом этапе данные о характеристиках $B_{\{l\}}^{прим}$ условий проведения информационной операции.

Математическая постановка задачи обоснования рационального сценария $\Lambda_{\langle n\rangle}^{p(прим)}$ целевого применения СИБ на пятом этапе имеет следующее выражение:

$$\Lambda_{\langle n\rangle}^{p(прим)} = \underset{A_{\langle n\rangle}^{прим} \in \{A_{\langle n\rangle}^{\partial}\}}{arg} \left\{ P_Ц\left(A_{\langle n\rangle}^{прим}\left(\Delta_{\langle n\rangle}^{p(экс)}\right); A_{\langle k''\rangle}^{\prime\prime прим}\right) \geq P_Ц^{ТР} / \right. \quad (16)$$

$$\left. / \left(C_5\left(A_{\langle n\rangle}^{прим}\left(\Delta_{\langle n\rangle}^{p(экс)}\right); A_{\langle k''\rangle}^{\prime\prime прим}\right) \leq C_5^{П}\right) \cap \left(T_5\left(A_{\langle n\rangle}^{прим}\left(\Delta_{\langle n\rangle}^{p(экс)}\right); A_{\langle k''\rangle}^{\prime\prime прим}\right) \leq T_5^{Д}\right) \right\},$$

где $\Lambda_{\langle n\rangle}^{p(прим)}$ – рациональный сценарий целевого применения СИБ (характеризуемой параметрами $A_{\langle k'\rangle}^{\prime(изг)}$), полученный на основе обработки оперативной информации $I\left({}_5A_{\langle k''\rangle}^{\prime\prime прим}\right), I\left({}_5B_{\langle l\rangle}^{прим}\right)$.

Замечание 8. Процесс обоснования рационального сценария $\Lambda_{\langle n\rangle}^{p(прим)}$, обеспечивающего требуемую $P_Ц^{ТР}$ условную вероятность $P_Ц$ выполнения задачи целевого применения СИБ, подразумевает под собой проведение обеспечивающими системами «рефлексивного контроля» [21, 22, 27] предполагаемого нарушителя в условиях ограничений на предельную $C_5^{П}$ стоимость C_5 и директивные $T_5^{Д}$ затраты времени T_5 на организацию и ведение мониторинга.

Замечание 9. Для адаптивных СИБ по мере получения информации о среде информационного конфликта производится:

– корректировка значений управляемых $A_{\langle k'_У\rangle}^{\prime\, p(изг)У}$ параметров $A_{\langle k'\rangle}^{\prime\, p(изг)}$, $A_{\langle k'\rangle}^{\prime\, p(изг)У} \subseteq A_{\langle k'\rangle}^{\prime\, p(изг)}$;

– обоснование рационального сценария $\Lambda_{\langle n\rangle}^{p(прим)}$ из фиксированной области $\left\{\Lambda_{\langle m\rangle}^{прим}\left(A_{\langle k''\rangle}^{\prime\prime(прим)}\right)\right\}$.

Замечание 10. Для проактивных СИБ на этом этапе производится (по мере получения информации о среде информационного конфликта) расширение области $\left\{\Lambda_{\langle m\rangle}^{прим}\right\}$, то есть генерирование новых сценариев $\Lambda_{\langle m\rangle}^{*}$ целевого применения СИБ, не предусмотренных на этапе ВНУПР:

$$\left\{\Lambda_{\langle m\rangle}^{прим}\right\}^{*} = \left\{\Lambda_{\langle m\rangle}^{прим}\right\} \cup \Lambda_{\langle m\rangle}^{*}. \quad (17)$$

Проведенный выше анализ специфики итерационного внешнего проектирования облика проактивных СИБ позволил разработать модель итерационного системно-агрегативного внешнего проектирования облика проактивных СИБ, представленную на рисунке 2.

8. Обоснование степени функционально-технической (оперативной) готовности системы

Степень неопределенности будущих условий реализации ПрРеш обуславливает неопределенность (случайность) векторов $\hat{П}_{i\langle 3\rangle}$ и $\hat{П}_{i\langle 3\rangle}^{\partial}$. Тогда для i-ого этапа ЖЦС степень P_i реализуемости ПрРеш определяется (вычисляется) следующим показателем:

$$P_i = P\left(\hat{П}_{i\langle 3\rangle} \in \{\hat{П}_{i\langle 3\rangle}^{\partial}\}\right) \simeq$$

$$\simeq P\left[\left(\hat{P}_Ц \geq \hat{P}_Ц^{ТР}\right) \cap \left(\hat{C}_i \leq \hat{C}_i^{П}\right) \cap \left(\hat{T}_i \leq \hat{T}_i^{Д}\right)\right], \quad (18)$$

где $\wedge$ – символ случайной величины.

В результате показатель $P_{ДЦ}^{C}$ реализуемости ПрРеш с учетом итерационного характера этапа ВНЕПР СИБ примет следующее выражение:

$$P_{ДЦ}^{C} = \prod_{i=1}^{5} P_i = \prod_{i=1}^{5} P\left(\hat{П}_{i_{\langle 3\rangle}} \in \{\hat{П}_{i\langle 3\rangle}^{\partial}\}\right), \quad (19)$$

где P_1 – вероятность реализуемости ПрРеш на этапе ВНЕПР – вероятность события $\hat{A}$; P_2 – условная вероятность реализуемости ПрРеш на этапе ВНУПР – вероятность события $\hat{B}$ при условии A; P_3 – условная вероятность реализуемости ПрРеш на этапе изготовления СИБ – вероятность события $\hat{C}$ при условии $A \cap B$; P_4 – условная вероятность реализуемости ПрРеш на этапе эксплуатации СИБ – вероятность события $\hat{D}$ при условии $C \cap (A \cap B)$; P_5 – условная вероятность реализуемости ПрРеш на этапе организации и управления процессом целевого применения СИБ – вероятность события $\hat{E}$ при условии $D \cap (C \cap (A \cap B))$.

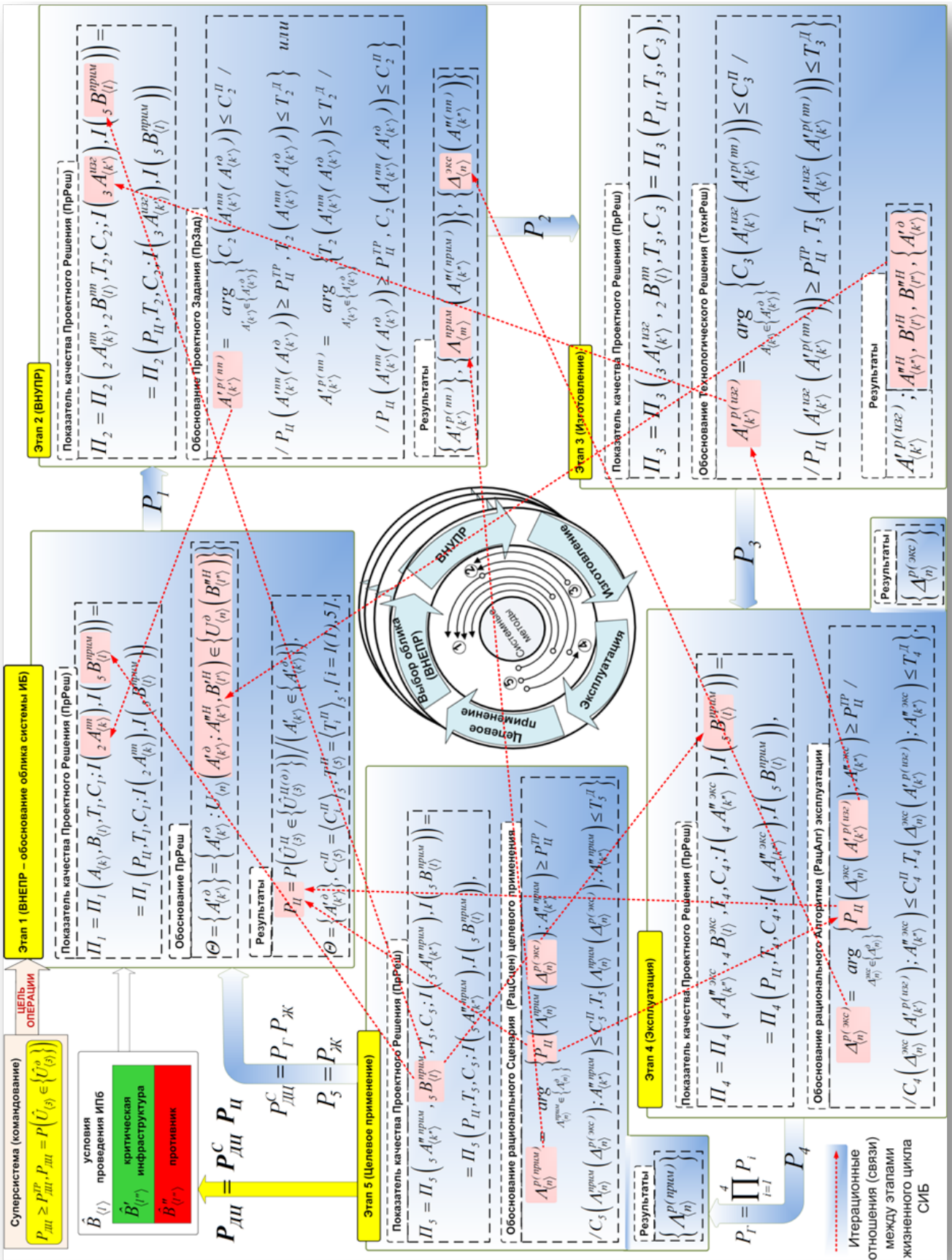

Рис. 2. *Модель итерационного системно-агрегативного ВНЕПР облика проактивных СИБ*

Пусть $P_{Ц} = P\left(\hat{U}^{Ц}_{\langle 3\rangle} \in \{\hat{U}^{Ц(\partial)}_{\langle 3\rangle}\}\right)$ – условная вероятность того, что цель проводимой СИБ операции будет достигнута – вероятность события $\hat{F}$ при условии $E \cap (D \cap (C \cap (A \cap B)))$, где $\hat{U}^{Ц}_{\langle 3\rangle}$ – вектор «целевых характеристик» процесса функционирования СИБ; $\{\hat{U}^{Ц(\partial)}_{\langle 3\rangle}\}$ – область допустимых значений «целевых (операционных) характеристик» процесса, то есть результатов процесса функционирования СИБ (целевого эффекта $\hat{v}$ и расходуемых ресурсов $\hat{r}, \hat{\tau}$), обеспечивающих достижение цели операции.

Тогда показатель $P_{ДЦ}$ эффективности применения СИБ примет следующее выражение:

$$P_{ДЦ} = P\left(\hat{\Pi}_{\langle 3\rangle} \in \left\{\hat{\Pi}^{\partial}_{\langle 3\rangle}\right\}\right) P\left(\hat{U}^{Ц}_{\langle 3\rangle} \in \left\{\hat{U}^{Ц(\partial)}_{\langle 3\rangle}\right\}\right) = P^{C}_{ДЦ}\, P_{Ц}, \quad (20)$$

где $\hat{\Pi}_{\langle 3\rangle}$ – вектор «обеспечивающих характеристик» целевого применения СИБ (вектор характеристик ПрРеш с учетом ЖЦС);

$\left\{\hat{\Pi}^{\partial}_{\langle 15\rangle}\right\} = \left\{\hat{\Pi}^{\partial}_{1\langle 3\rangle}\right\} \times \left\{\hat{\Pi}^{\partial}_{2\langle 3\rangle}\right\} \times \left\{\hat{\Pi}^{\partial}_{3\langle 3\rangle}\right\} \times \left\{\hat{\Pi}^{\partial}_{4\langle 3\rangle}\right\} \times \left\{\hat{\Pi}^{\partial}_{5\langle 3\rangle}\right\}$ – область допустимых значений вектора $\hat{\Pi}_{\langle 3\rangle}$

Целевые и обеспечивающие ЭТХ подробно рассмотрены в работе [25]. Обратим внимание, что поскольку $F \subset (E \cap D \cap C \cap A \cap B)$, то есть

$$\left(\hat{U}^{Ц}_{\langle 3\rangle} \in \left\{\hat{U}^{Ц(\partial)}_{\langle 3\rangle}\right\}\right) \subset \left(\hat{\Pi}_{\langle 3\rangle} \in \left\{\hat{\Pi}^{\partial}_{\langle 3\rangle}\right\}\right), \quad (21)$$

то вероятность $P_{ДЦ}$ – есть безусловная (априорная) вероятность случайного события $\hat{F} \cong \left(\hat{U}^{Ц}_{\langle 3\rangle} \in \{\hat{U}^{Ц(\partial)}_{\langle 3\rangle}\}\right)$, которое, таким образом, характеризует достижение цели операции исчерпывающе.

Замечание 11. Руководствуясь работой [25] и исходя из физического смысла сомножителей $P_i, [i = 1(1)4]$ их произведение $\prod_{i=1}^{4} P_i$ целесообразно называть показателем $P_{Г}$ готовности (эксплуатационно-технической готовности) СИБ к непосредственному применению:

$$P_{Г} = \prod_{i=1}^{4} P_i, \quad (22)$$

где $P_{Г}$ – вероятность того, что в момент начала операции СИБ будет готова к применению.

Замечание 12. Вероятность P_5 целесообразно обозначить через $P_{Ж}$ и называть показателем живучести СИБ:

$$P_5 = P_{Ж}, \quad (23)$$

где $P_{Ж}$ – условная вероятность того, что в ходе операции параметры и ЭТХ СИБ будут находиться в пределах, обеспечивающих выполнение ее задачи при любых воздействиях на нее окружающей среды (понимаемой в широком смысле, включая противника).

Замечание 13. Произведение $P_{Г}P_{Ж}$ целесообразно называть показателем функционально-технической (оперативной) готовности СИБ:

$$P^{C}_{ДЦ} = P_{Г}\, P_{Ж}, \quad (24)$$

где $P^{C}_{ДЦ}$ – показатель реализуемости ПрРеш с учетом жизненного цикла СИБ.

Замечание 14. Вероятность $P_{Ц}$ целесообразно называть условной вероятностью выполнения задачи системой.

Выводы

В настоящее время существующая методология проектирования СИБ по ряду причин относится без должного внимания к этапу ВНЕПР. Необходимость и важность этапа ВНЕПР СИБ состоит в том, что с помощью моделей макроуровня (относительно этапа конструирования) удается определить класс пригодных СИБ (при создании систем) и класс пригодных целенаправленных процессов (при организации применения СИБ), то есть в дальнейшем рассматривать не все возможные варианты создания системы и все возможные варианты организации ЦнПФС, а только пригодные.

Стоит отметить, что в условиях ограничений на выделенные ресурсы не всегда возможно создать проактивную СИБ требуемого качества. Для разрешения этого конфликта необходимо реализовать итерационный подход, то есть реализовать обратные связи между этапами и подэтапами жизненного цикла СИБ, что в настоящее время при ВНЕПР данных проактивных систем не реализуется.

Проведенный научно-технический анализ специфики задач, решаемых в ходе проектирования СИБ, позволил обосновать концептуальную схему итерационного системно-агрегативного ВНЕПР облика проактивных СИБ. Выявленные на основе данной схемы итерационные связи между этапами ЖЦС позволили разработать модель итерационного ВНЕПР облика проактивных СИБ.

Проведенные на модели исследования специфики итерационного ВНЕПР облика проактивных СИБ позволили:

– формально описать специфику функционирования СИБ, наделенных свойством проактивностью;

– обосновать показатель реализуемости ПрРеш с учетом итерационного характера этапа ВНЕПР проактивной системы ИПб в условиях неполноты знаний об условиях проведения информационной конфликта;

– для СИБ обосновать показатель готовности системы к непосредственному применению, показатели живучести и функционально-технической (оперативной) готовности.

Полученные результаты являются необходимым условием разработки адекватных методов:

– оценивания эффективности процесса функционирования проактивных СИБ, в том числе и уникальных;

– оценивания качества ПрРеш при разработке СИБ.

Вышесказанное позволит на этапе ВНЕПР спрогнозировать качество создаваемой СИБ, синтезировать пригодный облик данной системы и выработать обоснованные ПрРеш с учетом особенностей противоборства в киберпространстве.

Достоверность и обоснованность результатов, представленных в статье, подтверждается:

– всесторонним анализом предшествующих научных работ в области квалиметрии и теории эффективности целенаправленных процессов, привлечением базовых научных дисциплин и апробированного математического аппарата для формализации задачи итерационного обоснования качества ПрРеш на создание СИБ;

– корректностью постановки задачи обеспечения гарантируемого уровня потенциальной результативности целевого применения проектируемых СИБ и обоснованной декомпозицией этой задачи по этапам ЖЦС СИБ;

– строгостью формализации показателя реализуемости ПрРеш с учетом итерационного характера этапа ВНЕПР СИБ, показателя функционально-технической (оперативной) готовности системы;

– непротиворечивостью и совпадением частных результатов исследований с результатами работ других авторов.

Рецензент: *Еремеев Михаил Алексеевич, доктор технических наук, профессор института комплексной безопасности и специального приборостроения ФГБОУ ВО «Московский технологический институт», г. Москва, Россия. E-mail: mae1@rambler.ru*

Литература

1. Котенко И. В., Саенко И. Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. № 24. С. 21–40.
2. Котенко И. В., Саенко И. Б., Чернов А. В., Бутакова М. А. Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта // Труды СПИИРАН. 2013. № 30. С. 7–25.
3. Городецкий В.И., Карсаев О.В., Самойлов В.В., Серебряков С.В. Прикладные многоагентные системы группового управления // Искусственный интеллект и принятие решений. 2009. № 2. С. 3-24.
4. Карсаев О.В., Конюший В.Г. Многоагентные системы и средства их разработки // Труды СПИИРАН. 2009. Вып. 8. С. 234-254.
5. Городецкий В. И., Тушканова О. Н. Ассоциативная классификация: аналитический обзор. Часть 1 // Труды СПИИРАН. 2015. № 38. С. 183–203.
6. Городецкий В. И., Тушканова О. Н. Ассоциативная классификация: аналитический обзор. Часть 2 // Труды СПИИРАН. 2015. № 39. С. 212–240.
7. Троцкий Д. В. , Городецкий В. И. Сценарная модель знаний и язык описания процессов для оценки и прогнозирования ситуаций // Труды СПИИРАН. 2009. № 8. С. 94–127.
8. Котенко И. В., Саенко И. Б., Юсупов Р. М. Новое поколение систем мониторинга и управления инцидентами безопасности // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. 2014. № 3 (198). С. 7–18.
9. Котенко И. В., Саенко И. Б., Полубелова О. В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. № 25. С. 113–134.
10. Зегжда П.Д., Зегжда Д.П., Печенкин А.И., Полтавцева М.А. Моделирование информационных систем для решения задачи управления безопасностью // Проблемы информационной безопасности. Компьютерные системы. 2016. № 3. С. 7-16.
11. Зегжда П.Д., Зегжда Д.П., Степанова Т.В. Подход к построению обобщенной функционально-семантической модели кибербезопасности // Проблемы информационной безопасности. Компьютерные системы. 2015. № 3. С. 17-25.
12. Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография / Под общей редакцией С. Ф. Боева. – Университет Иннополис. Иннополис: «Издательский Дом «Афина», 2017. 440 с.
13. Левкин И.М., Володина А.А. Агрегированная операционно-временная модель оценивания эффективности отражения информационных угроз в больших информационных системах // Изв. вузов. Приборостроение. 2016. Т. 59, № 5. С. 335-341.
14. Глыбовский П.А., Глухов А.П., Пономарев Ю.А., Шиленков М.В. Подход к оцениванию и прогнозированию уровня защищенности информационных и телекоммуникационных систем // Труды СПИИРАН. 2015. № 5 (42). С. 180-195.
15. Рогозин Е.А., Попов А.Д. Постановка задач оценки эффективности при проектировании систем защиты информации от несанкционированного доступа в автоматизированных системах ОВД на основе новых информационных технологий // Общественная безопасность, законность и правопорядок в III тысячелетии. 2016. № 1-2. С. 359-361.
16. Львович Я.Е., Яковлев Д.С. Оптимизация проектирования систем защиты информации в автоматизированных информационных системах промышленных предприятий // Вестник Воронежского государственного университета инженерных технологий. 2014. № 2 (60). С. 90-94.

17. Дровникова И.Г., Рогозин Е.А., Никитин А.А. Методика проектирования систем информационной безопасности в автоматизированных системах // Технологии техносферной безопасности. 2016. № 4 (68). С. 262-267.
18. КоробкинД.И.,РогозинЕ.А.Модельоценкиэффективностипрограммнойсистемызащитыинформациивавтоматизированной системы на начальном этапе проектирования // Наукоемкие технологии в космических исследованиях Земли. 2014. Т. 6. № 5. С. 72-74.
19. Горбачев И.Е., Глухов А.П. Моделирование процессов нарушения информационной безопасности критической инфраструктуры // Труды СПИИРАН. 2015. № 1(38). С. 112-135.
20. Eremeev M.A., Gorbachev I.E. On using the stochastic superindicator for information security evaluation in automated systems // Automatic Control and Computer Sciences. 2015. Т. 49. № 8. pp. 653-658.
21. Горбачев И.Е., Кудрявцев А.Ю. Принципы рефлексивного управления нарушителем в инфотелекоммуникационных системах на основе технологии маскирования информационных ресурсов // Защита информации. Инсайд. 2015. № 1(61). С. 2-8.
22. Горбачев И.Е., Аниканов Г.А. Подход к снижению риска дезорганизации функционирования критической инфраструктуры в условиях информационного конфликта // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2(62). С. 106-119.
23. Юсупов Р.М., Мусаев А.А. Особенности оценивания эффективности информационных систем и технологий // Труды СПИИРАН. 2017. № 2 (51). С. 5-34.
24. Петухов Г.Б. Основы теории эффективности целенаправленных процессов. Часть 1. Методология, методы, модели. – СПб.: МО СССР, 1989. 660 с.
25. Петухов Г.Б., Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. – М.: АСТ, 2006. 504 с.
26. Горбачев И.Е., Еремеев М.А., Андрушкевич Д.В. Принципы оценивания потенциала нарушителя и результативности его информационных воздействий в инфотелекоммуникационных системах // Защита информации. Инсайд. 2014. № 6(60). С. 56-64.
27. Lavrova D.S., Pavlenko E.Y., Pechenkin A.I. Reflexive control over intruder using deception systems // Nonlinear Phenomena in Complex Systems. 2014. Т. 17. № 3. pp. 263-271.

THE CONCEPT OF EXTERNAL ITERATIONDESIGN APPEARANCE A PROACTIVE SYSTEMS INFORMATION SECURITY

I. Gorbachev[2]

Abstract. *In the work the analysis of unresolved problems that lead to the degeneration of the tasks of the external design of information security systems. The conceptual diagram of the iterative system–aggregate (external design) of modern systems of information security, which conducted a formal statement of the problem of providing a guaranteed level of potential impact the targeted application of the designed systems endowed with the property of being proactive. The formal definition of the design and appearance of the information security systems. Identified on the basis of this scheme the iterative connection between the phases of the life cycle of the system made it possible to develop iterative external design appearance of proactive information security systems. A feature of the model is reasonable for each stage of the life cycle of the system indicators quality design solutions, as well as reasonable goals for each iteration. The study made it possible to formally describe the specifics of the operation of information security systems endowed with the property proactive and to formulate an indicator of the feasibility of design solutions and to justify the increased system readiness for immediate use, indicators of survivability and functional–technical (operational) readiness.*

Keywords: *system information security efficiency estimation of iterative external design, proactivity, project design, indicator of the feasibility of the project lifecycle.*

References

1. Kotenko I. V., Saenko I. B. Arhitektura sistemy intellektual'nyh servisov zashhity informacii v kriticheski vazhnyh infrastrukturah, Trudy SPIIRAN [Works CPIIRAN], 2013, No 24, pp. 21-40.
2. Kotenko I. V., Saenko I. B., Chernov A. V., Butakova M. A. Postroenie mnogourovnevoj intellektual'noj sistemy obespechenija informacionnoj bezopasnosti dlja avtomatizirovannyh sistem zheleznodorozhnogo transporta, Trudy SPIIRAN [Works CPIIRAN], 2013, No 30, pp. 7-25.

2 Igor Gorbachev, Ph.D., Associate Professor of department «System for collecting and processing information», Federal State Establishment «Mozhaisky Military Aerospace Academy», St.-Petersburg, Russia: E-mail: gie1976@mail.ru

3. Gorodeckij V.I., Karsaev O.V., Samojlov V.V., Serebrjakov S.V. Prikladnye mnogoagent-nye sistemy gruppovogo upravlenija, Iskusstvennyj intellekt i prinjatie reshenij [Artificial intelligence and decision making], 2009, No 2, pp. 3-24.
4. Karsaev O.V., Konjushij V.G. Mnogoagentnye sistemy i sredstva ih razrabotki, Trudy SPIIRAN [Works CPIIRAN], 2009, No 8, pp. 234-254.
5. Gorodeckij V. I., Tushkanova O. N. Associativnaja klassifikacija: analiticheskij obzor. Chast' 1, Trudy SPIIRAN [Works CPIIRAN], 2015, No 38, pp. 183-203.
6. Gorodeckij V. I., Tushkanova O. N. Associativnaja klassifikacija: analiticheskij obzor. Chast' 2, Trudy SPIIRAN [Works CPIIRAN], 2015, No 39, pp. 212-240.
7. Trockij D. V. , Gorodeckij V. I. Scenarnaja model' znanij i jazyk opisanija processov dlja ocenki i prognozirovanija situacij, Trudy SPIIRAN [Works CPIIRAN], 2009, No 8, pp. 94-127.
8. Kotenko I. V., Saenko I. B., Jusupov R. M. Novoe pokolenie sistem monitoringa i uprav-lenija incidentami bezopasnosti, Nauchno-tehnicheskie vedomosti SPbGPU. Informatika. Telekommunikacii. Upravlenie [Nauchno-tekhnicheskie Vedomosti SPbGPU. Informatics. Telecommunications. Management.], 2014, No 3 (198), pp. 7-18.
9. Kotenko I. V., Saenko I. B., Polubelova O. V. Perspektivnye sistemy hranenija dannyh dlja monitoringa i upravlenija bezopasnost'ju informacii, Trudy SPIIRAN [Works CPIIRAN], 2013, No 25, pp. 113-134.
10. Zegzhda P.D., Zegzhda D.P., Pechenkin A.I., Poltavceva M.A. Modelirovanie informaci-onnyh sistem dlja reshenija zadachi upravlenija bezopasnost'ju, Problemy informacionnoj bezopasnosti. Komp'juternye sistemy [Information Security Problems. Computer Systems], 2016, No 3, pp. 7-16.
11. Zegzhda P.D., Zegzhda D.P., Stepanova T.V. Podhod k postroeniju obobshhennoj funkcio-nal'no-semanticheskoj modeli kiberbezopasnosti, Problemy informacionnoj bezopasnosti. Komp'juternye sistemy [Information Security Problems. Computer Systems], 2015, No 3, pp. 17-25.
12. Petrenko S. A., Stupin D. D. Nacional'naja sistema rannego preduprezhdenija o komp'ju-ternom napadenii: nauchnaja monografija / By ed. S. F. Boev. – Universitet Innopolis. Innopolis, Izdatel'skij Dom «Afina», 2017. 440 p.
13. Levkin I.M., Volodina A.A. Agregirovannaja operacionno-vremennaja model' ocenivanija jeffektivnosti otrazhenija informacionnyh ugroz v bol'shih informacionnyh sistemah, Izv. vuzov. Priborostroenie [Izv. universities. Instrumentation], 2016, No 5. pp. 335-341.
14. Glybovskij P.A., Gluhov A.P., Ponomarev Ju.A., Shilenkov M.V. Podhod k ocenivaniju i prognozirovaniju urovnja zashhishhennosti informacionnyh i telekommunikacionnyh sistem, Trudy SPIIRAN [Works CPIIRAN], 2015, No 5 (42), pp. 180-195.
15. Rogozin E.A., Popov A.D. Postanovka zadach ocenki jeffektivnosti pri proektirovanii sistem zashhity informacii ot nesankcionirovannogo dostupa v avtomatizirovannyh sistemah OVD na osnove novyh informacionnyh tehnologij, Obshhestvennaja bezopasnost', zakonnost' i pravoporjadok v III tysjacheletii [Public security, law and order in the third Millennium], 2016, No 1-2, pp. 359-361.
16. L'vovich Ja.E., Jakovlev D.S. Optimizacija proektirovanija sistem zashhity informacii v avtomatizirovannyh informacionnyh sistemah promyshlennyh predprijatij, Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernyh tehnologij [Herald of the Voronezh state University of engineering technologies], 2014, No 2 (60), pp. 90-94.
17. Drovnikova I.G., Rogozin E.A., Nikitin A.A. Metodika proektirovanija sistem informacionnoj bezopasnosti v avtomatizirovannyh sistemah, Tehnologii tehnosfernoj bezopasnosti [Technology of technosphere safety], 2016, No 4 (68), pp. 262-267.
18. Korobkin D.I., Rogozin E.A. Model' ocenki jeffektivnosti programmnoj sistemy zashhity informacii avtomatizirovannoj sistemy na nachal'nom jetape proektirovanija, Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli [Science intensive technologies in space research Land], 2014, No 5, pp. 72-74.
19. Gorbachev I.E., Gluhov A.P Modelirovanie processov narushenija informacionnoj bezopasnosti kriticheskoj infrastruktury, Trudy CPIIRAN [Works CPIIRAN], 2015, No 1(38), pp. 112-135.
20. Eremeev M.A., Gorbachev I.E. On using the stochastic superindicator for information security evaluation in automated systems // Automatic Control and Computer Sciences. 2015. T. 49. № 8. pp. 653-658.
21. Gorbachev I. E., Kudryavtsev A. Yu. Principy refleksivnogo upravlenija narushitelem v infotelekommunikacionnyh sistemah na osnove tehnologii maskirovanija informacionnyh resursov, Zashhita informacii. Insajd [Protection of information. INSIDE], 2015, No 1 (61), pp. 2-8.
22. Gorbachev I.E., Anikanov G.A. Podhod k snizheniju riska dezorganizacii funkcionirovanija kriticheskoj infrastruktury v uslovijah informacionnogo konflikta, Problemy informacionnoj bezopasnosti. Komp'juternye sistemy [Information Security Problems. Computer Systems]. 2015. No 2 (62). pp. 106-119.
23. Jusupov R.M., Musaev A.A. Osobennosti ocenivanija jeffektivnosti informacionnyh sistem i tehnologij, Trudy SPIIRAN [Works SPIIRAN], 2017, No 2 (51). pp. 5-34.
24. Petuhov G.B. Osnovy teorii jeffektivnosti celenapravlennyh processov. Chast' 1. Metodologija, metody, modeli. Uchebnik. – SPb.: MO SSSR, 1989, 660 p.
25. Petuhov G.B., Jakunin V.I. Metodologicheskie osnovy vneshnego proektirovanija celenapravlennyh processov i celeustremlennyh system. – M.: AST, 2006, 504 p.
26. Gorbachev I.E., Eremeev M.A., Andrushkevich D.V Principy ocenivanija potenciala narushitelja i rezul'tativnosti ego informacionnyh vozdejstvij v infotelekommunikacionnyh sistemah, Zashhita informacii. Insajd [Protection of information. INSIDE], 2014, No 6(60). pp. 56-64.
27. Lavrova D.S., Pavlenko E.Y., Pechenkin A.I. Reflexive control over intruder using deception systems // Nonlinear Phenomena in Complex Systems. 2014. T. 17. № 3. pp. 263-271.