ВЕСТНИК ВОЕННОГО ИННОВАЦИОННОГО ТЕХНОПОЛИСА «ЭРА», 2023, том 4, № 2, с. 184–189

ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

УДК 517.977.1

К ВОПРОСУ О РАЗРАБОТКЕ НАУЧНО-МЕТОДИЧЕСКОГО АППАРАТА ПРИМЕНЕНИЯ ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ПОДХОДА К АНАЛИЗУ И ОЦЕНКЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ АРХИТЕКТУРЫ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА СИСТЕМЫ НАВИГАЦИОННО-ГИДРОГРАФИЧЕСКОГО И ГИДРОМЕТЕОРОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ВОЕННО-МОРСКОГО ФЛОТА

© 2023 г. А. В. Ивкин[1,*], А. В. Жуков[1], О. В. Годовых[1], А. А. Потапов[1]

[1]НИЦ "Краснодарское высшее военное училище им. С.М. Штеменко", Краснодар, Россия

**E-mail: artemdtuproff@gmail.com*

Поступила в редакцию 06.07.2023 г.
После доработки 06.07.2023 г.
Принята к публикации 05.10.2023 г.

Представлена разработка научно-методического аппарата применения объектно-ориентированного подхода к анализу и оценке безопасности информационной архитектуры Единого информационного пространства (ЕИП) системы навигационно-гидрографического и гидрометеорологического обеспечения Военно-Морского Флота Мирового океана Министерства обороны Российской Федерации. Рассмотрены принципы объектно-ориентированного подхода и процессы построения модели классов. Проведены исследование информационной архитектуры и содержательный анализ безопасности ЕИП. Предложен подход к построению модельного обеспечения ЕИП.

DOI: 10.56304/S2782375X23020092

ВВЕДЕНИЕ

Информационная архитектура единого информационного пространства (**ЕИП**) представляет собой совокупность физических и абстрактных информационных объектов с их информационно-функциональными связями и предназначена для реализации функций обработки информации. В рамках общей научной задачи исследования математическое описание информационной архитектуры необходимо для построения формальных моделей ЕИП, позволяющих автоматизировать анализ и оценку защищенности информации проектируемых, модернизируемых и существующих систем, на основе предварительных результатов содержательного и объектно-ориентированного анализов. Предлагаемый подход к построению модельного обеспечения предполагает рассматривать формальные модели системы во взаимосвязи с содержательными моделями.

Предлагается новый подход к совместному моделированию процессов обработки и защиты геопространственной информации от несанкционированного доступа (**НСД**) в такой сложной информационной системе, как ЕИП, на основе применения взаимосвязанного трехуровневого представления процессов, что позволяет выделить объективно существующие между ними взаимосвязи при оценке безопасности информационной архитектуры рассматриваемого ЕИП.

Основными положениями такого подхода являются:

– для полного моделирования процессов обработки и защиты информации необходимо одновременно и совместно рассматривать процессы изменения физических, синтаксических и семантических состояний информационных объектов, выполняющих в системе функции обработки и защиты информации;

– для описания процесса изменения состояния каждого из рассматриваемых объектов применяются адаптированные методы объектно-ориентированного анализа сложных систем, теории входящих потоков задач и теории состояний ИРС [1–3];

– для установления взаимосвязи между процессами вводятся логические условия пребывания каждого объекта в одном из его состояний в зависимости от состояний других объектов.

Логические условия взаимосвязи процессов реализуются следующим образом:

– объект может находиться в заданном состоянии или изменять свое состояние в зависимости от заданных условий пребывания в соответствующем состоянии и от взаимодействия с другими взаимосвязанными объектами при нахождении их в заданном состоянии или при изменении этого состояния;

– модель взаимосвязанного трехуровневого процесса обработки и защиты информации представляет собой множество взаимосвязанных логическими условиями информационного взаимодействия процессов, имеющих физическую, синтаксическую или семантическую природу;

– модель представляется в виде трех взаимосвязанных ориентированных графов, вершинами которых являются состояния физических, синтаксических или семантических процессов, а дуги представляют собой направленные переходы из одного состояния в другое.

В работе формальное состояние системы S_w^t в момент времени t определяется как отражение множества физических и абстрактных модулей $\tilde{M}_w$ системы W на множество контролируемых $\tilde{Z}_w$ и смежных с ними неконтролируемых зон $\tilde{Z}_H$ всех уровней взаимодействия, а также множеством возможных отношений между активными абстрактными модулями $\tilde{M}_A^a$ и остальными модулями системы, которые определяются следующими кортежами парных интерфейсов модулей, находящихся в одной зоне в момент времени t:

$$S_w^t\left(\tilde{M}_w\right)=\left\{\tilde{Z}_w,\tilde{Z}_H,\tilde{M}_A^a\left(\tilde{F}_{x,i}^{\text{вых}}=\tilde{F}_{y,i}^{\text{вх}}\right),\right.$$
$$\left.\left(\tilde{L}_{x,j}^{\text{вых}}=\tilde{L}_{e,j}^{\text{вх}}\right),\left(C_{x,k}^{\text{вых}}=\tilde{C}_{y,k}^{вх}\right)|x\tilde{M}_A^a,\text{у}\in\tilde{M}_w\right\}, \quad (1)$$

где $S_w^t\left(\tilde{M}_w\right)$ – состояние системы W в момент времени I, состоящей из множества модулей; M_w – множество физических и абстрактных модулей, идентифицированных в системе W, $\tilde{M}_w$, $\subset \tilde{Z}_w$; $\tilde{Z}_w$ – множество контролируемых зон системы W; $\tilde{Z}_H$ – множество смежных зон, контролируемых системой W; $\tilde{M}_{\text{A}}^{\text{a}}$ – подмножество активных абстрактных модулей системы W на момент времени t, $\tilde{M}_{\text{A}}^{\text{a}}\subset M^a$; $(\tilde{F}_{x,i}^{\text{вых}}=\tilde{F}_{y,i}^{\text{вх}})$, $(\tilde{L}_{x,j}^{\text{вых}}=\tilde{L}_{e,j}^{\text{вх}})$, $(C_{x,k}^{\text{вых}}=\tilde{C}_{y,k}^{\text{вх}})$ – кортежи парных интерфейсов модулей, находящихся в одной зоне.

В процессе функционирования ЕИП (система W) под воздействием разных событий может сохранять или изменять свое состояние. Для отображения динамики процесса функционирования кроме множества формул состояний необходимо иметь множество формул, описывающих его переходы из одного состояния в другое.

В общем виде все возможные изменения или сохранения состояний ЕИП определяются отображением

$$\xi_w : S_w \to S_w. \quad (2)$$

Для каждого состояния S_W^n можно указать правила, позволяющие находить его образ $\xi_W^n\left(S_W^n\right)$ во множестве Sw. Упорядоченная последовательность правил ξ_W^n будет называться кортежем переходов. Кортеж переходов для S_W^n определяется как упорядоченная совокупность списков ξ_W^n, содержащих информацию о причинах перехода, номерах состояний, к которым выполняются переходы, и условия каждого перехода.

Под сменой состояния системы W здесь понимаются изменения в распределении или составе модулей относительно существующих контролируемых зон (**КЗ**), а также изменения информационных свойств модулей в результате потери или приобретения способности взаимодействовать через определенные открытые интерфейсы. Поэтому правила перехода состояний должны определять условия и причины, при которых возможны указанные события.

Все переходы происходят в результате воздействий активных алгоритмов на другие модули. Наличие в зоне активного алгоритма с кортежем интерфейсов, имеющим парные интерфейсы с другими объектами зоны, является причиной изменения состояния ЕИП. Условиями перехода является наличие шлюзов для соответствующих интерфейсов и ключей для их открытия.

Активные алгоритмы в общем случае могут воздействовать на физическое, синтаксическое или семантическое состояние модуля, перемещая его из одной зоны соответствующего уровня в другую или меняя состав его интерфейсов.

Возможность изменения состояния ЕИП в данный момент времени определяется следующими условиями:

– нахождением в одной КЗ модулей с одинаковыми парными интерфейсами;

– наличием хотя бы одного активного модуля.

Для примера информация о возможности и типе взаимодействия объектов номер 3 “Пользователь” (Π_3) и номер 25 “Синтаксический транслятор” (Тр_{25}) может быть описана выражением

$$\overline{\text{C}}_{3,25}\left(\dot{\Pi}_3,\text{Тр}_{25}\right)<=>\exists F\exists LC\left[F_{3,2,1}^{\text{вых}}=F_{25,2,1}^{\text{вх}}\wedge L_{3,2,1}^{\text{вых}}=L_{25,1,1}^{\text{вх}}\wedge C_{3,1}^{\text{вых}}=C_{25,1}^{\text{вх}}\right], \quad (3)$$

которое формализует следующую фразу: “Пользователь номер 3 ($П_3$) может вводить (копировать) информацию, набирая ее на клавиатуре $Тр_{25}$, если и только если у пользователя и клавиатуры существуют физические, синтаксические и семантические интерфейсы, такие что их номера совпадают, и при этом интерфейсы пользователя являются выходными, а клавиатуры – входными”.

Модель системы представляется в виде ориентированного графа, вершинами которого являются состояния процессов, а дуги представляют собой направленные переходы из одного состояния в другое.

Правила формализованного описания моделей состояний состоят из правил описания условий взаимодействия информационных объектов (модулей) и правил переходов [1].

Аксиома 1. Если два модуля M_x и My находятся в одной физической Z_F^f зоне и у них имеются парные физические интерфейсы $F_{x,k}^{вых} = F_{y,r}^{вх}$, то возможно их физическое взаимодействие I_F типа k^:

$$\begin{aligned} \bar{F} \equiv \forall_x \forall_y \forall I_F \left(M_x, M_y, k\right) <=> \\ <=> \exists k \exists f \left(F_{x,k}^{вых} = F_{e,k}^{вх} \middle| M_x, M_y \in Z_F^f\right), \end{aligned} \tag{4}$$

где $k \equiv \overline{1,n}$ – порядковый номер физического интерфейса в перечне типовых физических интерфейсов системы.

Аксиома 2. Если два модуля M_x и M_y одновременно находятся в одной физической Z_F^f и одной синтаксической Z_L^l зонах и у них имеются парные физические и синтаксические интерфейсы $F_{x,k}^{вых} = F_{y,k}^{вх}$ и $L_{x,k}^{вых} = L_{y,h}^{вх}$, то возможно их синтаксическое взаимодействие I_F типа h при условии выполнения k:

$$\left.\begin{aligned} \bar{L} \equiv \forall_x \forall_y \forall I_F \left(M_x, M_y, k\right) <=> \\ <=> \exists k \exists h \exists f \exists l \left(F_{x,k}^{вых} = F_{y,k}^{вх}\right) \wedge \\ \wedge\ L_{x,k}^{вых} = L_{y,h}^{вх} \middle| M_x, M_y \in Z_F^f, Z_L^l, \end{aligned}\right\} \tag{5}$$

где $h = \overline{1,m}$ – порядковый номер синтаксического интерфейса в перечне типовых синтаксических интерфейсов системы.

Аксиома 3. Если два модуля M_x и M_y одновременно находятся в одной физической Z_F^f, одной синтаксической Z_L^l и одной семантической Z_C^c зонах и у них имеются парные физические, синтаксические и семантические интерфейсы $F_{x,k}^{вых} = F_{y,k}^{вх}$, $L_{x,k}^{вых} = L_{y,h}^{вх}$, $F_{x,k}^{вых} = F_{y,k}^{вх}$ и $C_{x,g}^{вых} = C_{y,g}^{вх}$, то возможно их семантическое взаимодействие Ic при условии выполнения k и h:

$$\left.\begin{aligned} \bar{C} \equiv \forall_x \forall_y \forall I_C \left(M_x, M_y, g\right) <=> \\ <=> \exists k \exists h \exists g \exists c \left(F_{x,k}^{вых} = F_{y,k}^{вх}\right) \wedge \\ \wedge\ L_{x,k}^{вых} = L_{y,h}^{вх} \wedge C_{x,g}^{вх} = C_{y,g}^{вх} \middle| M_x, M_y \in Z_L^l, Z_C^c, \end{aligned}\right\} \tag{6}$$

где $g = \overline{1,p}$ – порядковый номер семантического интерфейса в перечне типовых семантических интерфейсов системы.

Правила формализованного описания переходов состояний системы заключаются в описании семантики возможных типов k, h и g информационных взаимодействий модулей на трех уровнях при выполнении аксиом 1, 2 и 3.

Аксиома 4. Семантика информационного взаимодействия на физическом уровне заключается в перемещении (трансляции) из физической зоны в смежную физическую зону $Z_F^f \to Z_F^{f,i}$ физического (носитель информации) или абстрактного (алгоритм или данные) модуля $A_{A,F}^y$ под воздействием активного модуля $M_a^x \in V\tilde{M}_{A,F}$ при выполнении условий $\bar{F}$ аксиомы 1.

Существуют два типа физического взаимодействия:

– перемещение *m-move* ($П_F$), при котором модуль M_{AF}^y оказывается в другой физической зоне Z_F^f:

$$\begin{aligned} \bar{m} \equiv \forall_x \forall_y \forall \Pi_F \left(M_a^x, M_{AF}^y, Z_F^f \to Z_F^{f,i}\right) <=> \\ <=> \exists x \exists y \left(\bar{F} \middle| M_a^x \in \tilde{M}_{A,F}\right); \end{aligned} \tag{7}$$

– копирование *c-copy*, т.е. размножение P_F модуля $M_{A,F}^y$ на 2, ..., n таких же модулей и их перемещение Π_F в f_i, ..., f_j зоны, при котором копии модуля $M_{AF}^{y_i,..y_n}$ оказываются в других зонах $Z_F^{f,i}$,..., $Z_F^{f,i}$. Эта операция обычно применяется к программным модулям:

$$\left.\begin{aligned} \bar{C} \equiv \forall_x \forall_y P_F \left(M_a^x, M_{A,F}^y \to M_{A,F}^{y_i,..y_n} \middle| M_{A,F}^y = M_{A,F}^{y_i,..y_n}\right) \Pi_F \left(M_a^x, M_{A,F}^{y_i,..y_n}\right), \\ Z_F^f \to Z_F^{f_i,..f_n} <=> \exists_x \exists_f \exists_i \exists_j \left(\bar{F} = l, M_a^x \in \tilde{M}_{A,F}, M_{A,F}^{y_i,..y_n} \in M_F^{f_i,..f_n}\right). \end{aligned}\right\} \tag{8}$$

Аксиома 5. Семантика информационного взаимодействия на синтаксическом уровне заключается в переводе синтаксиса *t-translation* абстрактного модуля M_A^y на другой язык, т.е. в перемещении Π_L его из одной синтаксической зоны в другую $Z_L^l = Z_L^{l,i}$ под воздействием активного синтаксического модуля транслятора T_L^x при выполнении условий $\bar{L}$ аксиомы 2:

$$\bar{t} \equiv \forall_x \forall_y \forall \Pi_L \left(T_L^x, M_A^y, Z_L^l \rightarrow Z_L^{l,i} \right) <=> \exists x \left(\bar{L} = l, T_L^x \tilde{M}_a \right). \quad (9)$$

Аксиома 6. Информационное взаимодействие на семантическом уровне заключается в активизации *a-action* активным модулем-алгоритмом M_a^x другого абстрактного модуля-алгоритма, т.е. в передаче управления Π_c в виде ресурсов и параметров модулям-алгоритмам, способным совершать операции $\bar{g}$, $\bar{d}$, $\bar{a}$, $\bar{m}$, $\bar{c}$, $\bar{t}$, при выполнении условий $\bar{c}$ аксиомы 3:

$$\bar{a} \equiv \forall_x \forall_y \forall \Pi_C \left(M_a^x, M_A^y, Z_C^c \rightarrow Z_C^{c,i} \left[\bar{g} \vee \bar{d} \vee \bar{a} \vee \bar{m} \vee \bar{c} \vee \bar{t} \right] \right) <=> \exists x \left(\bar{C} = l, M_a^x \tilde{M}_a \right). \quad (10)$$

Указанные операции определяют семантику возможностей модулей по исполнению следующих функций обработки информации на трех уровнях:

$\bar{g}$ – создание модуля, т.е. выделение носителя информации или его части под логическую структуру модуля, и идентификация в системе W новой структуры соответственно в качестве физического или абстрактного модуля;

$\bar{d}$ – уничтожение модуля, т.е. исключение носителя информации или логической структуры из системы W;

$\bar{a}$ – активизация модуля, т.е. передача ему управления;

$\bar{m}$ – физическое перемещение модуля, т.е. перемещение носителя информации как физического объекта или перемещение логической структуры как абстрактного объекта из одного носителя информации в другой;

$\bar{c}$ – физическое копирование модулей, т.е. выделение носителя информации под копию модуля, идентификация этого носителя и перемещение структуры модуля на выделенный носитель (создание и перемещение);

$\bar{t}$ – синтаксическая трансляция абстрактных модулей, т.е. изменение синтаксиса или алфавита модуля без изменения семантики.

Для каждого защищаемого модуля системы политикой безопасности должны быть определены КЗ, в которых он может находиться. КЗ могут задаваться способами, аналогичными применяемым в формальных моделях управления доступом, например дискреционной, мандатной или их комбинацией [1]. Так, в случае использования мандатной модели управления доступом, которая рекомендуется нормативно-руководящими документами для использования в ИРС [4], в информационную структуру системы вносится решетка ценности, которая делит объекты системы на иерархические уровни в зависимости от субъективно установленной ценности этих информационных ресурсов. КЗ для этой модели образуются уровнями иерархии решетки ценности.

Построение формальной модели информационной архитектуры ЕИП с целью автоматического поиска и доказательства наличия или отсутствия опасных траекторий информационного процесса может осуществляться на основе предложенной математической модели состояний системы W, процессов обработки и защиты данных.

В рамках поставленной цели математическая модель ЕИП должна учитывать и позволять моделировать отношения:

– между декларируемой политикой информационной безопасности D каждого участка ЕИП и реализованной политикой R, которая определяет возможности субъектов S (активных модулей) получать доступ к объектам Q (пассивным модулям) в ходе информационного процесса;

– между политиками информационной безопасности участков ЕИП, для которых определена отдельная политика, в том числе реализованная средствами и методами разных уровней информационного взаимодействия;

– между информационными объектами, для которых определена политика безопасности, и объектами, для которых она не определена, но имеющих типовые (стандартные) интерфейсы взаимодействия.

Для решения поставленных задач указанные отношения необходимо выявить и привести к нормальной форме, т.е. выразить в виде типовых атрибутов предикатов, описывающих взаимодействия.

$D(S, Q, atr)$ – предикат, истинный при условии, что субъект S имеет доступ к объекту Q с ат-

рибутом *atr* в декларируемой политике безопасности *D* участка ЕИП, которая зафиксирована в нормативно-руководящей документации, например в инструкции по режиму секретности или таблице разграничения доступа к системе управления ЕИП.

Атрибут *atr* может принимать значения создавать – $\overline{g}$, удалять – $\overline{d}$, перемещать – $\overline{m}$, копировать – $\overline{c}$ (перемещать копию модуля), транслировать синтаксис – $\overline{t}$, активизировать – $\overline{a}$.

R(*S*, *Q*, *atr*) – предикат, описывающий реальный доступ в систему, реализованный совокупностью физических *F*, синтаксических *L* и семантических *C* средств и методов защиты, которые определяются совокупностью всех правил разграничения доступа и интерфейсами модулей ЕИП, стандартных для них, но не учитываемых в политиках безопасности Центра.

Для упрощения записи используем обычно применяемые атрибуты чтение – *r*, запись – *w* и изменение – *ch*.

Тогда условие конфиденциальности информации описывается выражением

$$CON = \forall S \forall Q[R(S,Q,R)] \supset D(S,Q,R)], \qquad (11)$$

так как функция импликации истинна, если реально доступ есть и он разрешен, либо его нет, что доказывается эквивалентными преобразованиями

$$CON = \forall S \forall Q \left[\begin{array}{c} R(S,Q,r) \wedge D(S,Q,R) \vee \\ \vee\ \overline{R}(S,Q,R) \wedge D(S,Q,R) \vee D(S,Q,r) \end{array} \right] = \left. \begin{array}{c} \\ \\ \end{array} \right\} . \qquad (12)$$
$$= \forall S \forall Q \left[\begin{array}{c} R(S,Q,r) \wedge D(S,Q,r) \vee \\ \vee\ \overline{R}(S,Q,r) \end{array} \right]$$

Формула, описывающая нарушение конфиденциальности, получается инвертированием выражения (12):

$$\overline{CON} = \overline{\forall S \forall Q \left[\begin{array}{c} R(S,Q,r) \wedge D(S,Q,R) \vee \\ \vee\ \overline{R}(S,Q,R) \end{array} \right]} = \left. \begin{array}{c} \\ \\ \end{array} \right\} . \qquad (13)$$
$$= \exists S \exists Q [R(S,Q,r) \wedge D(S,Q,r) \vee]$$

Для политики безопасности, принятой в системе Windows NT, атрибут “Изменение” – *ch* “покрывает” атрибут “Чтение” – *r*, поэтому для указанной политики выражение (13) примет вид

$$CON = \exists S \exists Q[R(S,Q,R)] \wedge R(S,Q,ch)] \wedge \wedge\ \overline{D}(S,Q,ch). \qquad (14)$$

Выражение (14) является исходным логическим выражением для построения программы, моделирующей соответствие декларируемой и реальной политик информационной безопасности.

Логическое выражение для вычисления предиката $R(S,Q,ch)$ имеет вид

$$R(S,Q,ch) = D_t(S,Q,atr) \vee \vee\ R_l(S,Q_l,atr), D_t(S,Q,atr), \qquad (15)$$

что соответствует высказыванию “доступ субъекта *S* к объекту *Q* имеется, если он есть в таблице разграничения доступа либо он возможен через другие уровни взаимодействия через субъект *S*1. Этот дополнительный путь описывается через логическое выражение

$$R1(S,S1,atr) = RF(S,S1,atr) \vee RT(S,S1,atr), \qquad (16)$$

где предикат *RT* означает условие транзитивности передачи доступа через субъект *S*1 и описывается в общем случае формальным выражением

$$RT(S1,S2,atr) = = RF(S1,Sn,atr) \vee RT(Sn,S2,atr). \qquad (17)$$

Условие доступности информации определяется через введенные определения предикатов выражением

$$ACC = \forall S \forall Q[D(S,Q,r)] \supset R(S,Q,r). \qquad (18)$$

Доказательством служат следующие эквивалентные преобразования:

$$\left. \begin{array}{c} \forall S \forall Q[D(S,Q,r) \supset R(S,Q,R)] = \\ = \forall S \forall Q[D(S,Q,r) \wedge R(S,Q,R) \vee \overline{R}(S,Q,r) \wedge \\ \wedge\ \overline{D}(S,Q,r) \wedge R(S,Q,r)] = \\ = [R(S,Q,r) \wedge D(S,Q,r) \vee \overline{D}(S,Q,r)]. \end{array} \right\} \qquad (19)$$

Нарушение доступности по чтению описывается отрицанием выражения (20):

$$\left. \begin{array}{c} \overline{ACC} = \overline{\left[\begin{array}{c} R(S,Q,r) \wedge D(S,Q,R) \vee \\ \overline{D}(S,Q,R) \end{array} \right]} = \\ = \{[\overline{R}(S,Q,r) \vee \mathrm{x}\overline{D}(S,Q,R)\,\mathrm{xx}D(S,Q,R)]\} \\ = \exists S \exists Q[D(S,Q,r) \wedge R(S,Q,r)]. \end{array} \right\} \qquad (20)$$

Для доступности по записи выражение (20) можно представить в виде

$$\overline{ACC} = \forall S \forall Q[D(S,Q,w)] \supset \overline{R}(S,Q,w). \qquad (21)$$

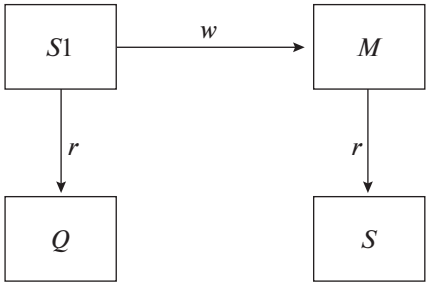

Рис. 1. Опосредованный доступ к объекту Q через память.

Для примера в политике безопасности Windows NT выражение (21) примет вид

$$\overline{ACC} = \forall S \forall Q[D(S,Q,r)] \wedge \overline{R}(S,Q,ch) \vee \vee D(S,Q,ch) \wedge \overline{R}(S,Q,ch). \quad (22)$$

Условие целостности информации в той части, которая определяется разграничением доступа (без функций хранения, архивирования и т.п.), описываются выражением

$$\left.\begin{aligned}\overline{SAF} = \overline{\forall S \forall Q[R(S,Q,w) \supset D(S,Q,w)]}. = \\ = \forall S \forall Q[R(S,Q,w) \wedge \\ \wedge D(S,Q,w) \vee \overline{R}(S,Q,w)].\end{aligned}\right\} \quad (23)$$

что соответствует высказыванию: “Целостность объекта Q обеспечивается, если декларируемый и реальный доступы к объекту Q субъекта S эквивалентны или реальный доступ отсутствует”.

Отсутствие целостности описывается отрицанием выражения (24):

$$\left.\begin{aligned}\overline{SAF} = \overline{\forall S \forall Q[R(S,Q,w) \wedge D(S,Q,w)]}. = \\ = ESEQ[R(S,Q,w) \wedge \overline{D}(S,Q,w)].\end{aligned}\right\} \quad (24)$$

Формальное выражение (24) соответствует высказыванию “декларируется отсутствие доступа S к объекту Q, хотя реально доступ по записи w существует”.

Доступ субъекта S к объекту Q может быть проведен через память M с помощью другого субъекта $S1$. Геометрическое отображение такой связи показано на рис. 1.

Графическое отображение рис. 1 можно описать следующим формальным выражением:

$$\left.\begin{aligned}R(S,Q,r) = D_t(S,Q,r) \wedge R_s(S1,Q,M); \\ R_s(S,Q,M) = D_t(S,Q,r) \wedge D_t(S,M,w).\end{aligned}\right\} \quad (25)$$

В общем виде “скрытый доступ” через память может быть описан выражением

$$R_s(S,Q,r) = D_t(S,M,r) \wedge R_t(S1,Q,M) \quad (26)$$

при $R_m(S,Q_1,Q_2,) = D_t(S,Q_1,r) \wedge D_t(S,Q_1,w) \vee D_t(S,Q_2,w) \wedge D_t(S,Q_3,w) \vee R_m(S_1,Q_1,Q_2)$, где $R_m(S,Q,M)$ – предикат транзитивности доступа через память.

Выражение (26) является логическим выражением для программы, моделирующей “скрытые” каналы утечки информации, которые можно обнаружить на этапе формирования политики информационной безопасности.

ЗАКЛЮЧЕНИЕ

Разработанный математический аппарат формализации состояний ЕИП, процессов обработки и защиты данных позволяет повысить достоверность оценки защищенности геопространственной информации от НСД за счет автоматизации процедур анализа системы и поиска опасных траекторий информационного процесса, приводящих ее в состояние НСД, учета большего количества существенных для безопасности информации отношений между объектами и охвата оценки всей технологической цепочки обработки информации. В целом разработанный научно-методический аппарат может быть основой для совершенствования методического обеспечения оценки защищенности геопространственной информации от НСД в ЕИП.

СПИСОК ЛИТЕРАТУРЫ

1. *Аполлонский С.М.* Моделирование и расчет электромагнитных полей в технических устройствах. М.: Русайнс, 2019. Т. 1. 320 с.
2. *Краснов М.Л.* Обыкновенные дифференциальные уравнения: Задачи и примеры с подробными решениями. М.: Ленанд, 2019. 256 с.
3. *Сикорский Ю.С.* Обыкновенные дифференциальные уравнения с приложением их к некоторым техническим задачам. М.: КомКнига, 2019. 156 с.
4. *Яглом И.М.* Математические структуры и математическое моделирование. М.: Ленанд, 2018. 144 с.
5. *Тельнов Ю.Ф.* Информационные системы и технологии. М.: Юнити, 2017. 544 с.
6. Об утверждении национального стандарта: приказ ФСТЭК России от 27 декабря 2006 г. № 373-ст. Стандартинформ, 2020.
7. *Шаньгин В.Ф.* Информационная безопасность и защита информации. М.: ДМК-Пресс, 2019. 702 с.
8. *Остроух А.В.* Интеллектуальные информационные системы и технологии. СПб.: Лань, 2019. 308 с.
9. *Шумов В.В.* Государственная и общественная безопасность. Моделирование и прогнозирование. М.: Ленанд, 2017. 144 с.