УДК 004.78.056:51–7

А.С. Дубровин, В.И. Сумин, Ю.Ю. Громов, В.М. Тютюнник

Системный подход к обеспечению безопасности в автоматизированной информационной системе специального назначения

Рассмотрена математическая модель подсистемы обеспечения безопасности в автоматизированной информационной системе специального назначения, иерархически декомпозируемой по уровням безопасности, на основе которой возможно разрабатывать и анализировать сравнительно гибкие правила разграничения доступа к информации с высокой гарантированностью их выполнения с помощью аппарата конечных нелинейных решеток. Предложены две подходящие для этого конечные нелинейные решётки. Для каждой из них определены носитель, частичная упорядоченность и алгебраические операции. Даны интерпретации этих решеток, как векторных уровней безопасности, в отличие от известной интерпретации конечных линейных решеток, как числовых уровней безопасности. Для векторных уровней безопасности определены правила «нет чтения вверх» и «нет записи вниз» мандатной политики безопасности. Обоснована эквивалентность моделирующих возможностей этих решёток. Разработанная модель интегрирует принципы мандатного и дискреционного методов контроля доступа, рассматривая субъекты в роли посредников между пользователями и объектами. Представлена модель Белла-ЛаПадулы, адаптированная к формализации уровней безопасности конечными нелинейными решётками.

Ключевые слова: *системный подход, подсистема обеспечения безопасности информации, автоматизированная информационная система специального назначения, решётка, уровень безопасности, правила разграничения доступа, дискреционная политика безопасности, мандатная политика безопасности*

DOI: 10.36535/0548-0027-2025-02-3

ВВЕДЕНИЕ

Автоматизированная информационная система специального назначения (АИС СН) управляет информационными ресурсами в особых условиях [1], которые отличаются критичностью и требуют повышенного уровня надёжности и защищённости не только АИС СН, но и используемых в ней средств вычислительной техники[1]. Высокозащищённые классы АИС обязаны управлять информационными потоками с помощью дискреционных меток конфиденциальности, а используемые в них компьютеры должны поддерживать мандатный принцип контроля доступа. Сочетание дискреционных и мандатных правил разграничения доступа обеспечивает комплексный контроль доступа к информации, объединяя контроль единичных актов доступа с управлением информационными потоками. Основополагающую роль в этом играет назначение субъектам и объектам классификационных уровней безопасности путём присвоения им классификационных меток конфиденциальности.

Таким образом, одна из характерных особенностей АИС СН – необходимость обеспечения безопасности информации в ней посредством подсистемы, управляющей комплексным доступом (включая управление информационными потоками) к информации, организованной иерархическим образом через распределение пользователей, субъектов и объектов по уровням безопасности. Именно такой подход к

[1] Гостехкомиссия России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: руководящий документ. – Москва: Военное изд-во, 1992. – 39 с.; Гостехкомиссия России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: руководящий документ. – Москва: Военное изд-во, 1992. – 24 с.

обеспечению безопасности информации на основе системного подхода даёт более высокую гарантированность защиты информации за счёт привлечения к анализу защищённости АИС СН доказательной базы, присущей математическим моделям мандатной политики безопасности в отличие от математических моделей дискреционной политики безопасности, традиционно формализующих контроль доступа субъектов к защищаемым ресурсам согласно матрице доступа. Так возникает проблематика математического моделирования подсистемы обеспечения безопасности информации в АИС СН, иерархически декомпозируемой по уровням безопасности. Такое моделирование призвано максимально удовлетворить взаимно противоречивые требования к защищённости информации и к гибкости правил разграничения доступа, ведь именно в этой гибкости мандатная политика безопасности уступает дискреционной.

Одним из направлений одновременного обеспечения высокой защищённости информации и максимальной гибкости правил разграничения доступа к иерархически организованным ресурсам АИС СН является использование проблемно-ориентированного математического аппарата эталонной модели защищенной автоматизированной системы (ЭМЗАС) [2-6]. Этот математический аппарат развивался как альтернатива традиционному математическому аппарату решёток [7]. Доказано, что в общем случае множество уровней безопасности в АИС СН должно представлять собой решётку [8]. Однако практическое распространение в реальных АИС СН получили лишь линейные решётки, т. е. цепи. В результате востребованным оказался лишь тривиальный частный случай теории решёток – теория упорядоченных множеств (цепей) [9]. При этом частичная упорядоченность множеств усекается до линейной, т.е. совершенной упорядоченности. Негативным последствием такого усечения является искусственно ограниченная гибкость правил разграничения доступа, которую можно усилить переходом от линейных решеток к нелинейным.

Отсюда вытекает цель настоящего исследования: на основе системного подхода разработать такую математическую модель подсистемы обеспечения безопасности информации в АИС СН, иерархически декомпозируемой по уровням безопасности, на основе которой удобно разрабатывать и анализировать гибкие правила разграничения доступа к информации с высокой гарантированностью их выполнения за счёт использования математического аппарата нелинейных решёток.

ПОСТАНОВКА ЗАДАЧИ

Пусть задано базовое множество L уровней безопасности АИС СН, причём $L \neq \emptyset$, $|L| < +\infty$. Это множество можно рассматривать в качестве носителя некоторой алгебраической системы Λ_L в универсальной алгебре, снабдив его соответствующей сигнатурой, которая в общем случае задаёт на L набор операций и набор отношений. Тогда алгебраическая система Λ_L представляет собой само множество уровней безопасности АИС СН. Для единообразного представления уровней безопасности АИС СН один из указанных наборов удобно принимать пустым, что приводит к двум эквивалентным взглядам на множество Λ_L: 1) как на модель (пустой набор операций), 2) как на алгебру (пустой набор отношений). Естественное для уровней безопасности отношение – частичное нестрогое отношение порядка $\leq$ для элементов множества L, обладающее свойствами рефлективности, антисимметричности и транзитивности (отношение $(l_1 \leq l_2)$ или, что то же самое, $(l_2 \geq l_1)$, где $l_1, l_2 \in L$, означает не более высокую безопасность уровня l_1 по сравнению с уровнем l_2 или, что то же самое, не менее высокую безопасность уровня l_2 по сравнению с l_1):

$$(\forall l \in L)(l \leq l); \tag{1}$$

$$(\forall l_1, l_2 \in L | l_1 \leq l_2 \wedge l_2 \leq l_1)(l_1 = l_2); \tag{2}$$

$$(\forall l_1, l_2, l_3 \in L | l_1 \leq l_2 \wedge l_2 \leq l_3)(l_1 \leq l_3). \tag{3}$$

Рассматривая множество Λ_L как частично упорядоченное, можно определить для любого непустого подмножества $\tilde{L} \subseteq L$ супремум (sup) и инфинум (inf), если они существуют, или установить факт несуществования:

$$\begin{gathered}(sup(\tilde{L}) = l) \Leftrightarrow \\ \Leftrightarrow \left((\forall l' \in \tilde{L}) \begin{pmatrix} (l' \leq l) \wedge (\forall l'' \in L | l'' \leq l) \\ (\exists l''' \in \tilde{L})(l''' \leq l'') \end{pmatrix} \right);\end{gathered} \tag{4}$$

$$\begin{gathered}(inf(\tilde{L}) = l) \Leftrightarrow \\ \Leftrightarrow \left((\forall l' \in \tilde{L}) \begin{pmatrix} (l' \geq l) \wedge (\forall l'' \in L | l'' \geq l) \\ (\exists l''' \in \tilde{L})(l''' \geq l'') \end{pmatrix} \right).\end{gathered} \tag{5}$$

Очевидно, что если $|\tilde{L}| = 1$, то в силу (1), (4) и (5), имеем:

$$(l \in \tilde{L}) \Rightarrow (sup(\tilde{L}) = inf(\tilde{L}) = l). \tag{6}$$

Если $|L| = 1$, то соответствующее множество Λ_L означает фактически отсутствие иерархической декомпозиции АИС СН по уровням безопасности. Цели настоящего исследования отвечает только случай $2 \leq |L| < +\infty$. При $|\tilde{L}| = 2$ можно обозначить $\tilde{L} = \{l_1, l_2\}$, тогда формулы (4) и (5) принимают вид:

$$\begin{gathered}(sup(\tilde{L}) = sup\{l_1, l_2\} = l) \Leftrightarrow \\ \Leftrightarrow \left((l_1, l_2 \leq l) \wedge (\forall l' \in L | l' \leq l)(l' \leq l_1 \vee l' \leq l_2) \right);\end{gathered} \tag{7}$$

$$\begin{gathered}(inf(\tilde{L}) = inf\{l_1, l_2\} = l) \Leftrightarrow \\ \Leftrightarrow \left((l \leq l_1, l_2) \wedge (\forall l' \in L | l' \leq l_1 \wedge l' \leq l_2)(l' \leq l) \right).\end{gathered} \tag{8}$$

Множество Λ_L является решёткой тогда и только тогда, когда

$$(\forall \tilde{L} \subseteq L | |\tilde{L}| = 2)(\exists\, sup(\tilde{L}), inf(\tilde{L})), \tag{9}$$

причём в (9) можно эквивалентным образом заменить $|\tilde{L}| = 2$ на $1 \leq |\tilde{L}| \leq |L|$.

Выражения (1)-(9) описывают решётку Λ_L уровней безопасности АИС СН как модель. Для перехода от этого описания к описанию той же самой решётки Λ_L, но уже как алгебры, введём две алгебраические бинарные операции (сложение $\vee$ и умножение $\wedge$) следующим образом:

$$\left(\forall l', l'' \in L\right)\begin{pmatrix}\left(l' \vee l'' = sup\{l', l''\}\right) \wedge \\ \wedge \left(l' \wedge l'' = inf\{l', l''\}\right)\end{pmatrix}. \quad (10)$$

При этом выполнено:

$$\left(\forall l', l'' \in L \middle| l' \le l''\right)\left(\left(l' \wedge l'' = l'\right) \wedge \left(l' \vee l'' = l''\right)\right). \quad (11)$$

Введённые по формуле (10) с выполнением формулы (11) алгебраические бинарные операции $\vee$ и $\wedge$ удовлетворяют алгебраическим свойствам идемпотентности, коммутативности, ассоциативности и поглощения:

$$(\forall l \in L)\left((l \vee l = l) \wedge (l \wedge l = l)\right); \quad (12)$$

$$\left(\forall l', l'' \in L\right)\left(\left(l' \vee l'' = l'' \vee l'\right) \wedge \left(l' \wedge l'' = l'' \wedge l'\right)\right); \quad (13)$$

$$\left(\forall l', l'', l''' \in L\right)\begin{pmatrix}\left(\left(l' \vee l''\right) \vee l''' = l' \vee \left(l'' \vee l'''\right)\right) \wedge \\ \wedge \left(\left(l' \wedge l''\right) \wedge l''' = l' \wedge \left(l'' \wedge l'''\right)\right)\end{pmatrix}; \quad (14)$$

$$\left(\forall l', l'' \in L\right)\begin{pmatrix}\left(l' \wedge \left(l' \vee l''\right) = l'\right) \wedge \\ \wedge \left(l' \vee \left(l' \wedge l''\right) = l'\right)\end{pmatrix}. \quad (15)$$

Выражения (12)-(15) описывают решётку Λ_L уровней безопасности АИС СН как алгебру. Для перехода от этого алгебраического описания к описанию той же самой решётки Λ_L, но уже как модели, введём две бинарные операции (супремум sup и инфинум inf) по формуле (10); при этом опять выполнено условие (11). При рассмотрении решётки Λ_L уровней безопасности АИС СН как модели и при рассмотрении её как алгебры имеет место изоморфизм решёток, но эти два изоморфизма совпадают.

Иерархическая декомпозиция АИС СН по уровням безопасности L решётки Λ_L производится в рамках субъектно-объектной модели [10] АИС СН функцией уровня безопасности $F_L: X \to L$, $X = S \cup O$, где S – множество субъектов, O – множество объектов. Эта функция в общем случае необратима как функция, но при её рассмотрении как отображения общего вида обратное ему отображение $F_L^{-1}: L \to X$ задаёт классы безопасности X_i (где $i = \overline{1, |L|}$) сущностей АИС СН (субъектов и объектов), удовлетворяющие формулам:

$$\bigcup_i X_i = X;\ X_i \cap X_j = \emptyset,\ i \ne j;$$
$$\left(\forall i = \overline{1, |L|}\right)(\forall x \in X_i)(F_L(x) = l_i \in L). \quad (16)$$

Итог иерархической декомпозиции АИС СН по уровням безопасности L представляет собой удовлетворяющие (16) классы безопасности X_i.

В простейшем частном случае решётка $\Lambda_{L_0(N)}$ уровней безопасности АИС СН имеет носитель

$$L_0(n) = \{1,2, \dots, n\},\ 2 \le |L_0(n)| = n < +\infty \quad (17)$$

из последовательных натуральных чисел, начиная с единицы, а отношение $\le$ для $\Lambda_{L_0(n)}$ представляет собой обычное отношение «меньше или равно» для натуральных чисел. Типовой пример такой организации уровней безопасности АИС СН – решётка $\Lambda_{L_0(5)}$ с носителем $L_0(5) = \{1,2,3,4,5\}$, элементы которого интерпретируются следующим образом: 1 – отсутствие грифа, 2 – гриф «для служебного пользования», 3 – гриф «секретно», 4 – гриф «совершенно секретно», 5 – гриф «особой важности».

Решётка $\Lambda_{L_0(n)}$ с носителем $L_0(n)$, определённым из выражения (17), представляет собой простейший пример конечной линейной решётки (конечной цепи), т. е. такого конечного частично упорядоченного множества $\Lambda_{\bar{L}(n)}$, у которого все элементы носителя

$$\bar{L}(n) = \{l_1, l_2, \dots, l_n\},\ 2 \le |\bar{L}(n)| = n < +\infty \quad (18)$$

попарно сравнимы:

$$\left(\forall l_1, l_2 \in \bar{L}(n)\right)(l_1 \le l_2 \vee l_2 \le l_1). \quad (19)$$

Как и решётка $\Lambda_{L_0(n)}$, решётка $\Lambda_{\bar{L}(n)}$, определённая выражениями (18) и (19), подходит для формализованного описания уровней безопасности АИС СН, но не вносит ничего нового в это описание, так как для данного n эти решётки изоморфны. Поэтому любая решётка $\Lambda_{\bar{L}(n)}$ может быть представлена решёткой $\Lambda_{L_0(n)}$ установлением эквивалентности элементов носителей $\bar{L}(n), L_0(n)$: $l_i \leftrightarrow i$, так что $\left(l_i \le l_j\right) \Leftrightarrow (i \le j)$.

Ситуация радикально меняется при переходе от конечных линейных решёток $\Lambda_{L_0(n)}$, $\Lambda_{\bar{L}(n)}$ к конечным нелинейным, так как они уже не изоморфны конечным линейным решёткам, а потому способны внести нечто новое в формализованное описание уровней безопасности АИС СН – идею неполной попарной их сравнимости, которая означает то, что не все, а лишь некоторые пары уровней сравнимы. При использовании математического аппарата нелинейных решёток в качестве основы для математического моделирования сложной системы обеспечения безопасности информации в АИС СН, иерархически декомпозируемой по уровням безопасности, сохраняется присущая математическим моделям мандатной политики безопасности высокая гарантированность выполнения правил разграничения доступа к информации, но существенно повышается гибкость этих правил за счёт возможности существенно более сложного упорядочения уровней безопасности.

Поэтому требуется разработать такую математическую модель, которая реализовала бы эту возможность с помощью системного подхода [11, 12].

ТЕОРЕТИЧЕСКИЙ АНАЛИЗ

Классический пример нелинейной решётки – решётка Λ_F с носителем

$$F = \{f | f: [0,1] \to \mathbb{R}\}, \quad (20)$$

в которой частичная упорядоченность $\leq$ и алгебраические операции $\vee$ и $\wedge$ заданы следующими выражениями [9]:

$$(\forall f, g \in F)\left(\begin{matrix}(f \leq g) \Leftrightarrow \\ \Leftrightarrow \big((\forall t \in [0,1])\big(f(t) \leq g(t)\big)\big)\end{matrix}\right); \quad (21)$$

$$(\forall f, g \in F)(\forall t \in [0,1])\left(\begin{matrix}f(t) \vee g(t) = \\ = sup\{f(t), g(t)\} = \\ = max\big(f(t), g(t)\big)\end{matrix}\right); \quad (22)$$

$$(\forall f, g \in F)(\forall t \in [0,1])\left(\begin{matrix}f(t) \wedge g(t) = \\ = inf\{f(t), g(t)\} = \\ = min\big(f(t), g(t)\big)\end{matrix}\right). \quad (23)$$

Однако решётка Λ_F, заданная выражениями (20)-(23), хотя и обладает перспективными для дальнейшего теоретического анализа отношением (21) и операциями (22) и (23), всё же не подходит для формализованного описания уровней безопасности АИС СН, так как эта решетка не конечна, а мощность её носителя F, заданного выражением (20), даже больше мощности континуума. Неподходящий носитель F, заданный выражением (20), можно заменить подходящим носителем $\bar{L}(n)$, заданным выражением (18) в его расширенной (за счёт представления каждого элемента итогового носителя некоторой заданной мощности $N \in N$ в виде вектора-столбца одного и того же размера $M \in N$) форме

$$\bar{L}(M,N) = \{\boldsymbol{l}_1, \boldsymbol{l}_2, \dots, \boldsymbol{l}_N\}, \boldsymbol{l}_j = \big(l_{1j}, l_{2j}, \dots, l_{Mj}\big)^T,$$
$$l_{ij} \in \bar{L}(n), i = \overline{1,M}, j = \overline{1,N}, \quad (24)$$

перейдя, тем самым, от бесконечной нелинейной решётки Λ_F к конечной нелинейной решётке $\tilde{\Lambda}_{\bar{L}(M,N)}$, частичная упорядоченность $\leq$ и алгебраические операции $\vee$ и $\wedge$ в которой заданы следующими выражениями, полученными необходимой адаптацией выражений (21)-(23) к другому носителю (24):

$$\big(\forall \boldsymbol{l}_{j_1}, \boldsymbol{l}_{j_2} \in \bar{L}(M,N)\big)\left(\begin{matrix}\big(\boldsymbol{l}_{j_1} \leq \boldsymbol{l}_{j_2}\big) \Leftrightarrow \\ \Leftrightarrow \begin{pmatrix}(\forall i \in \mathbb{N} | 1 \leq i \leq M) \\ \big(l_{ij_1} \leq l_{ij_2}\big)\end{pmatrix}\end{matrix}\right); \quad (25)$$

$$\big(\forall \boldsymbol{l}_{j_1}, \boldsymbol{l}_{j_2} \in \bar{L}(M,N)\big)\,(\forall i \in \mathbb{N} | 1 \leq i \leq M)$$
$$\big(\boldsymbol{l}_{j_1} \vee \boldsymbol{l}_{j_2} = sup\{\boldsymbol{l}_{j_1}, \boldsymbol{l}_{j_2}\} = max\big(l_{ij_1}, l_{ij_1}\big)\big); \quad (26)$$

$$\big(\forall \boldsymbol{l}_{j_1}, \boldsymbol{l}_{j_2} \in \bar{L}(M,N)\big)\,(\forall i \in \mathbb{N} | 1 \leq i \leq M)$$
$$\big(\boldsymbol{l}_{j_1} \vee \boldsymbol{l}_{j_2} = inf\{\boldsymbol{l}_{j_1}, \boldsymbol{l}_{j_2}\} = min\big(l_{ij_1}, l_{ij_1}\big)\big). \quad (27)$$

Очевидно, что в выражении (24) для устранения избыточности уровней безопасности АИС СН следует полагать

$$\big(\forall \boldsymbol{l}_{j_1}, \boldsymbol{l}_{j_2} \in \bar{L}(M,N)\big)\big(\boldsymbol{l}_{j_1} \neq \boldsymbol{l}_{j_2}\big). \quad (28)$$

Аналогично неподходящий носитель F, заданный выражением (20), можно заменить другим подходящим носителем $L_0(n)$, заданным выражением (17), в его расширенной в том же смысле форме $L_0(M,N)$, перейдя от бесконечной нелинейной решётки Λ_F к конечной нелинейной решётке $\tilde{\Lambda}_{L_0(M,N)}$, при этом выражения (24)-(28) остаются в силе с заменой в них $\bar{L}(n)$ на $L_0(n)$.

Величины l_{ij}, $i = \overline{1,M}$, $j = \overline{1,N}$, определяющие носитель $\bar{L}(M,N)$ или $L_0(M,N)$ решётки $\tilde{\Lambda}_{\bar{L}(M,N)}$ или $\tilde{\Lambda}_{L_0(M,N)}$ в соответствии с (24) без замены в ней $\bar{L}(n)$ на $L_0(n)$ или с таковой заменой, составляют матрицу $\bar{\boldsymbol{L}}_{M\times N} = \|l_{ij}\|_{M\times N}$, $i = \overline{1,M}$, $j = \overline{1,N}$, столбцами которой служат векторы-столбцы $\boldsymbol{l}_j$, $j = \overline{1,N}$ в роли элементов носителя:

$$\bar{\boldsymbol{L}}_{M\times N} = \sum_{j=1}^{N} \boldsymbol{l}_j \boldsymbol{e}_j{}^T,$$
$$\boldsymbol{e}_j = \big(e_j^k\big) = \|e_j^k\|_{1\times N}, e_j^k = \delta_{jk}, k = \overline{1,N}, \quad (29)$$

где: $\boldsymbol{e}_j$, $j = \overline{1,N}$ – стандартный базис в R^N;
δ_{jk} – символ Кронекера.

Обратный переход от матрицы $\bar{\boldsymbol{L}}_{M\times N}$, определенной в (29), к вектор-столбцам $\boldsymbol{l}_j$, $j = \overline{1,N}$, производится по формуле

$$\boldsymbol{l}_j = \bar{\boldsymbol{L}}_{M\times N} \boldsymbol{e}_j, j = \overline{1,N}. \quad (30)$$

По аналогии с матрицей доступа дискреционной политики безопасности матрицу $\bar{\boldsymbol{L}}_{M\times N}$, определённую выражением (29), естественно назвать мандатной матрицей доступа. Каждый её столбец как отдельный целостный вектор, определённый выражением (30), заменяет уровень безопасности (обычно числовой, причём, как правило, в виде натурального числа), определённый в математических моделях мандатной политики безопасности, основанных на использовании математического аппарата конечных линейных решёток (цепей) вида $\Lambda_{L_0(N)}$ или $\Lambda_{\bar{L}(N)}$. Аналогично тому, как в упомянутых моделях те или иные уровни безопасности присваиваются как защищаемым объектам (тогда они являют собой метки конфиденциальности), так и пользователям АИС СН (тогда они являют собой степени доверия им), при переходе к использованию предлагаемого математического аппарата конечных нелинейных решёток вида $\tilde{\Lambda}_{L_0(M,N)}$ или $\tilde{\Lambda}_{\bar{L}(M,N)}$ те или иные столбцы мандатной матрицы доступа как вектор-столбцы тоже присваиваются как защищаемым объектам (тогда они являют собой векторные метки конфиденциальности), так и пользователям АИС СН (тогда они являют собой векторные степени доверия им). Тем самым, переход от конечных линейных решёток к конечным

нелинейным решёткам при формализации правил разграничения доступа к ресурсам АИС СН приводит к переходу от числовых к векторным уровням безопасности.

При этом сразу возникает вопрос о подходящей интерпретации векторных уровней безопасности (причём отдельно для векторных меток конфиденциальности и для векторных степеней доверия) тем более что такая интерпретация неоднозначна. Подходящим ориентиром здесь может служить классическая интерпретация матриц доступа дискреционной политики безопасности, согласно которой строки соответствуют пользователям или субъектам, выступающим в качестве посредников между пользователями и объектами, столбцы – объектам, а элемент матрицы – характеристике прав доступа данного пользователя или субъекта к данному объекту. Одним из недостатков такой формализации неизбежно оказывается то, что пользователи и субъекты занимают в ней одно и то же место, хотя более адекватным представлением доступа пользователя к объекту является разделение этого доступа на две фазы или этапа: доступ пользователя к субъекту как к посреднику, и доступ субъекта как посредника к объекту. Векторный характер уровня безопасности вместо числового позволяет устранить данный недостаток следующим образом.

Так как векторные метки конфиденциальности присваиваются защищаемым объектам, то естественно ассоциировать их с доступом к объектам. Аналогично, так как векторные степени доверия присваиваются пользователям, то естественно ассоциировать их с доступом только пользователей, но не субъектов. Субъекты же, группируемые в соответствующие классы безопасности субъектов, естественно ассоциировать с элементами векторных уровней безопасности. Все классы безопасности субъектов взаимно не пересекаются, и каждый субъект принадлежит ровно одному из этих классов. Таким образом, величина M трактуется как количество классов безопасности субъектов в АИС СН, а индекс $i = \overline{1,M}$ в (24)-(27) – как номер класса безопасности субъектов. Векторный уровень безопасности $\boldsymbol{l}_j$ представляет собой набор M числовых уровней безопасности l_{ij}, $i = \overline{1,M}$. Если векторный уровень безопасности $\boldsymbol{l}_j$ присвоен объекту в качестве векторной метки конфиденциальности, то соответствующий числовой уровень безопасности l_{ij} интерпретируется как числовая метка конфиденциальности, которая присвоена объекту в отношении доступа к нему субъектов, относящихся к классу безопасности субъектов i. Если же векторный уровень безопасности $\boldsymbol{l}_j$ присвоен пользователю в качестве векторной степени доверия, то соответствующий числовой уровень безопасности l_{ij} интерпретируется, как числовая степень доверия, которая присвоена пользователю в отношении доступа его к субъектам, относящимся к классу безопасности субъектов i.

Иерархическая декомпозиция АИС СН по уровням безопасности $L_0(M,N)$ или $\bar{L}(M,N)$ нелинейных решёток $\tilde{\Lambda}_{L_0(M,N)}$ или $\tilde{\Lambda}_{\bar{L}(M,N)}$ соответственно производится в рамках субъектно-объектной модели [10] АИС СН функцией уровня безопасности (в данном случае уже не числового, а векторного) $F_{L_0(M,N)}: X \to L_0(M,N)$ или $F_{\bar{L}(M,N)}: X \to \bar{L}(M,N)$. В отличие от случая линейных решёток $\Lambda_{L_0(N)}$ или $\Lambda_{\bar{L}(N)}$, в котором аргумент X функции числового уровня безопасности представляется в виде $X = S \cup O$, где S – множество субъектов, O – множество объектов, в случае нелинейных решёток $\tilde{\Lambda}_{L_0(M,N)}$ или $\tilde{\Lambda}_{\bar{L}(M,N)}$ аргумент X функции векторного уровня безопасности представляется в виде $X = U \cup O$, где U – множество пользователей, O – множество объектов. Функция $F_{L_0(M,N)}$ или $F_{\bar{L}(M,N)}$ векторного уровня безопасности для случая нелинейных решёток $\tilde{\Lambda}_{L_0(M,N)}$ или $\tilde{\Lambda}_{\bar{L}(M,N)}$, как и функция $F_{L_0(n)}$ или $F_{\bar{L}(n)}$ числового уровня безопасности для случая линейных решёток $\Lambda_{L_0(N)}$ или $\Lambda_{\bar{L}(N)}$, в общем случае необратима как функция, но при её рассмотрении как отображения общего вида обратное ему отображение ${F_{L_0(M,N)}}^{-1}: L_0(M,N) \to X$ или ${F_{\bar{L}(M,N)}}^{-1}: \bar{L}(M,N) \to X$, как и обратное отображению $F_{L_0(n)}$ или $F_{\bar{L}(n)}$ отображение ${F_{L_0(n)}}^{-1}$ или ${F_{\bar{L}(n)}}^{-1}$, задаёт классы безопасности X_j тех сущностей АИС СН, которым присвоены уровни безопасности (в данном случае нелинейных решёток $\tilde{\Lambda}_{L_0(M,N)}$ или $\tilde{\Lambda}_{\bar{L}(M,N)}$ векторные уровни безопасности присваиваются уже не субъектам и объектам, как в случае линейных решеток $\Lambda_{L_0(N)}$ или $\Lambda_{\bar{L}(N)}$, субъектам и объектам присваиваются числовые уровни безопасности, причём $j = \overline{1,n}$, а пользователям и объектам, причём $j = \overline{1,N}$), удовлетворяющие выражениям:

$$\cup_{j=1}^{N} X_j = X;\ X_{j_1} \cap X_{j_2} = \emptyset,\ j_1 \neq j_2; \tag{31}$$

$$\left(\forall j = \overline{1,N}\right)\left(\forall x \in X_j\right) \left(F_{L_0(M,N)}(x) = \boldsymbol{l}_j \in L_0(M,N)\right); \tag{32}$$

$$\left(\forall j = \overline{1,N}\right)\left(\forall x \in X_j\right) \left(F_{\bar{L}(M,N)}(x) = \boldsymbol{l}_j \in \bar{L}(M,N)\right). \tag{33}$$

Итог иерархической декомпозиции АИС СН по уровням безопасности $L_0(M,N)$ или $\bar{L}(M,N)$ представляет собой классы безопасности X_j, удовлетворяющие выражениям (31)-(33) как частному случаю (16).

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Проведённый теоретический анализ позволяет специфицировать математическую модель подсистемы обеспечения безопасности информации в АИС СН, иерархически декомпозируемой по уровням безопасности, при переходе с математического аппарата конечных линейных решёток на математический аппарат конечных нелинейных решёток для обеспечения удобства разработки и анализа гибких правил разграничения доступа к информации с высокой гарантированностью их выполнения. Такой переход сопряжён с переходом от числовых уровней безопасности, присваиваемых субъектам в качестве числовых степеней доверия к ним и объектам в качестве их числовых меток конфиденциальности, к векторным уровням безопасности, присваиваемым пользователям в качестве векторных степеней доверия к ним и объектам в

качестве их векторных меток конфиденциальности. Правила “no read up” (NRU) и “no write down” (NWD) мандатной политики безопасности при этом остаются в силе с точностью до замены субъектов на пользователей и числовых уровней безопасности на векторные. Правило NRU принимает вид правила возможного наличия у данного пользователя с данной векторной степенью доверия права чтения информации из данного объекта с данной векторной меткой конфиденциальности только в том случае, когда она присвоена этому объекту в соответствии с векторным уровнем безопасности, который не выше того векторного уровня безопасности, в соответствии с которым присвоена данная векторная степень доверия данному пользователю. Правило NWD принимает вид правила возможного наличия у данного пользователя с данной векторной степенью доверия права записи информации в данный объект с данной векторной меткой конфиденциальности только в том случае, когда она присвоена ему в соответствии с векторным уровнем безопасности, который не ниже того векторного уровня безопасности, в соответствии с которым присвоена данная векторная степень доверия данному пользователю.

Правила NRU и NWD, сформулированные для случая использования математического аппарата конечных нелинейных решёток, формализуются следующим образом. Пусть пользователю присвоена степень доверия в виде векторного уровня безопасности $\boldsymbol{l}_{j_U} = \left(l_{1j_U}, l_{2j_U}, \dots, l_{Mj_U}\right)^T$, $j_U \in N$, $1 \le j_U \le N$, а данному объекту присвоена векторная метка конфиденциальности в виде векторного уровня безопасности $\boldsymbol{l}_{j_O} = \left(l_{1j_O}, l_{2j_O}, \dots, l_{Mj_O}\right)^T$, $j_0 \in N$, $1 \le j_O \le N$.

Тогда правило NRU утверждает, что пользователь может иметь право чтения информации из данного объекта только в том случае, когда $\boldsymbol{l}_{j_U} \ge \boldsymbol{l}_{j_O}$, а правило NWD утверждает, что данный пользователь может иметь право записи информации в данный объект только в том случае, когда $\boldsymbol{l}_{j_U} \le \boldsymbol{l}_{j_O}$. Далее, с использованием выражения (25), эти же правила NRU и NWD можно детализировать до числовых уровней безопасности следующим образом.

Согласно правилу NRU, у данного пользователя может присутствовать право чтения информации из данного объекта только в том случае, когда при чтении через посредничество любого субъекта, относящегося к каждому классу безопасности субъектов $i = \overline{1, M}$, числовой уровень безопасности, в соответствии с которым присвоена данная числовая степень доверия данному пользователю, не ниже числового уровня безопасности, в соответствии с которым присвоена данная числовая метка конфиденциальности данному объекту, т. е. справедливо неравенство $l_{ij_U} \ge l_{ij_O}$. Согласно правилу NWD, у данного пользователя может присутствовать право записи информации в данный объект только в том случае, когда при записи через посредничество любого субъекта, относящегося к каждому классу безопасности субъектов $i = \overline{1, M}$, числовой уровень безопасности, в соответствии с которым присвоена данная числовая степень доверия данному пользователю, не выше числового уровня безопасности, в соответствии с которым присвоена данная числовая метка конфиденциальности данному объекту, т. е. справедливо неравенство $l_{ij_U} \le l_{ij_O}$.

Согласно совместному применению правил NRU и NWD, данный пользователь может иметь права чтения информации из данного объекта и одновременно записи информации в данный объект только в том случае, когда одновременно выполнены условия $\boldsymbol{l}_{j_U} \ge \boldsymbol{l}_{j_O}$ и $\boldsymbol{l}_{j_U} \le \boldsymbol{l}_{j_O}$. В силу свойства (2) антисимметричности решеток это означает, что $\boldsymbol{l}_{j_U} = \boldsymbol{l}_{j_O}$, т.е. каждый объект доступен любому пользователю того же самого уровня безопасности, что и у объекта. Тем самым, случай $\boldsymbol{l}_{j_U} = \boldsymbol{l}_{j_O}$ выходит за пределы области применимости мандатного метода контроля доступа и подпадает под действие дискреционного метода (аналогичный факт имеет место и при использовании математического аппарата линейных решёток). Область применимости дискреционного метода опять лежит внутри каждого конкретного класса безопасности (в данном нелинейном случае – класса безопасности пользователей и объектов).

Важным отличием нелинейных решёток от линейных является отсутствие требования сравнимости любых двух элементов, в силу чего векторные уровни безопасности $\boldsymbol{l}_{j_U}$ и $\boldsymbol{l}_{j_O}$ необязательно сравнимы. В случае их несравнимости, у данного пользователя отсутствует как право чтения информации из данного объекта, так и право записи информации в данный объект. Так, согласно (25), для нелинейных решёток $\tilde{\Lambda}_{L_0(M,N)}$ и $\tilde{\Lambda}_{\bar{L}(M,N)}$ этот случай несравнимости $\boldsymbol{l}_{j_U}$ и $\boldsymbol{l}_{j_O}$ формализуется вплоть до детализации по числовым уровням безопасности следующим образом:

$$\begin{pmatrix}\left(\exists l_{j_U}, l_{j_O} \in L_0(M,N)\right) \\ \left(\left(\neg\begin{pmatrix}\left(l_{j_U} \le l_{j_O}\right) \vee \\ \vee \left(l_{j_U} \ge l_{j_O}\right)\end{pmatrix}\right) \Leftrightarrow \right. \\ \left. \Leftrightarrow \left(\begin{pmatrix}\left(\exists i_1, i_2 \in N | 1 \le i_1, i_2 \le M\right) \\ \left(l_{i_1 j_U} > l_{i_1 j_O} \wedge l_{i_2 j_U} < l_{i_1 j_O}\right)\end{pmatrix}\right)\end{pmatrix} \tag{34}$$

$$\begin{pmatrix}\left(\exists l_{j_U}, l_{j_O} \in \bar{L}(M,N)\right) \\ \left(\left(\neg\begin{pmatrix}\left(l_{j_U} \le l_{j_O}\right) \vee \\ \vee \left(l_{j_U} \ge l_{j_O}\right)\end{pmatrix}\right) \Leftrightarrow \right. \\ \left. \Leftrightarrow \left(\begin{pmatrix}\left(\exists i_1, i_2 \in N | 1 \le i_1, i_2 \le M\right) \\ \left(l_{i_1 j_U} > l_{i_1 j_O} \wedge l_{i_2 j_U} < l_{i_1 j_O}\right)\end{pmatrix}\right)\end{pmatrix} \tag{35}$$

Неравенство $l_{i_1 j_U} > l_{i_1 j_O}$ в (34) и (35) требует отсутствия у данного пользователя права записи информации в данный объект по причине того, что возможное посредничество субъекта из класса безопасности субъектов i_1 не гарантирует безопасности такого доступа. Неравенство $l_{i_2 j_U} < l_{i_1 j_O}$ в (34) и (35) требует отсутствия у данного пользователя права чтения информации из данного объекта по причине того, что возможное посредничество субъекта из класса безопасности субъектов i_2 не гарантирует без-

опасности такого доступа. В конечном счете, из этих двух требований вытекает, что действительно у данного пользователя отсутствует как право чтения информации из данного объекта, так и право записи информации в данный объект. При использовании же математического аппарата линейных решёток мандатный метод контроля доступа не даёт возможности установить полный запрет на доступ данного пользователя к данному объекту: и на чтение, и на запись. В этом проявляется одно из преимуществ использования математического аппарата нелинейных решёток вместо линейных.

Модель Белла-ЛаПадулы [8, 10], играющая важную роль при математическом моделировании подсистемы обеспечения безопасности информации в АИС СН, иерархически декомпозируемой по уровням безопасности, естественным образом адаптируется под переход на использование нелинейных решёток уровней безопасности вместо линейных. Так, вместо множества S субъектов в адаптированной модели Белла-ЛаПадулы фигурирует множество U пользователей. При этой адаптации множество O объектов и множество R прав доступа остаются инвариантными. В классическом варианте модели Белла-ЛаПадулы $R = \{read, write\}$. Соответственно замене S на U, матрица доступа для дискреционного метода контроля доступа внутри классов безопасности пользователей и объектов принимает вид $\boldsymbol{A}_{|U|\times|O|} = \|a_{uo}\|_{|U|\times|O|}$ вместо $\boldsymbol{A}_{|S|\times|O|} = \|a_{so}\|_{|S|\times|O|}$, где $u \in U$, $s \in S$, $o \in O$. Конечная линейная решётка $\Lambda_{L_0(N)}$ или $\Lambda_{\bar{L}(N)}$ числовых уровней безопасности $L_0(N)$ или $\bar{L}(N)$ субъектов и объектов АИС СН заменяется на конечную нелинейную решетку $\tilde{\Lambda}_{L_0(M,N)}$ или $\tilde{\Lambda}_{\bar{L}(M,N)}$ векторных уровней безопасности $L_0(M,N)$ или $\bar{L}(M,N)$ пользователей и объектов АИС СН. Соответственно замене решетки, функция $F_{L_0(N)}: S \cup O \to L_0(N)$ или $F_{\bar{L}(N)}: S \cup O \to \bar{L}(N)$ числового уровня безопасности субъектов и объектов АИС СН заменяется на функцию $F_{L_0(M,N)}: U \cup O \to L_0(M,N)$ или $F_{\bar{L}(M,N)}: U \cup O \to \bar{L}(M,N)$ векторного уровня безопасности пользователей и объектов АИС СН. Состояние подсистемы обеспечения безопасности информации в АИС СН, иерархически декомпозируемой по конечной нелинейной решётке $\tilde{\Lambda}_{L_0(M,N)}$ или $\tilde{\Lambda}_{\bar{L}(M,N)}$ векторных уровней безопасности $L_0(M,N)$ или $\bar{L}(M,N)$, определяется кортежем $\left(F_{L_0(M,N)}, \boldsymbol{A}_{|U|\times|O|}\right)$ или $\left(F_{\bar{L}(M,N)}, \boldsymbol{A}_{|U|\times|O|}\right)$ соответственно.

Все такие состояния образуют множество V, в котором особо выделяется начальное состояние $v_0 \in V$. Переход системы из одного состояния в другое происходит в результате запросов пользователей (а не субъектов) на проведение операций, трактуемое как доступ пользователей к объектам, причём все такие запросы образуют множество Q. При адаптации модели Белла-ЛаПадулы сохраняет свой общий вид функция переходов $F_T: (V \times Q) \to V$, согласно которой происходит переход системы из старого состояния $v \in V$ в новое состояние $v^* \in V$ при очередном запросе $q \in Q$ пользователя на доступ. В модели Белла-ЛаПадулы подсистема обеспечения безопасности информации в АИС СН представляется при такой адаптации кортежем $\Sigma = (v_0, Q, F_T)$.

Без ограничения общности будем считать, что выбрана решётка $\tilde{\Lambda}_{L_0(M,N)}$ векторных уровней безопасности $L_0(M,N)$. Безопасность относительно этой решётки данного состояния означает безопасность относительно неё же данного состояния одновременно и по чтению, и по записи (соблюдение в данном состоянии всеми пользователями обоих правил NRU и NWD). Безопасность относительно этой решётки данного состояния по чтению означает, что в этом состоянии каждый пользователь соблюдает правило NRU:

$$(\forall u \in U)(\forall o \in O | read \in a_{uo}) \left(F_{L_0(M,N)}(u) \geq F_{L_0(M,N)}(o)\right). \quad (36)$$

Аналогично, безопасность относительно этой решетки данного состояния по записи означает, что в нем каждый пользователь соблюдает правило NWD:

$$(\forall u \in U)(\forall o \in O | write \in a_{uo}) \left(F_{L_0(M,N)}(o) \geq F_{L_0(M,N)}(s)\right). \quad (37)$$

Критерий безопасности системы $\Sigma = (v_0, Q, F_T)$ в модели Белла-ЛаПадулы в своём общем виде инвариантен относительно выбора решётки уровней безопасности – безопасность состояния v_0 и всех из него достижимых за конечное число запросов из Q.

Основная теорема безопасности в модели Белла-ЛаПадулы гарантирует безопасность системы $\Sigma = (v_0, Q, F_T)$ с выбранной конечной нелинейной решёткой уровней безопасности (например, $\tilde{\Lambda}_{L_0(M,N)}$), если и только если обеспечена безопасность состояния v_0 и поддерживаются следующие ограничения на переходы $F_T(v,q) = v^*$, где $v = \left(F_{L_0(M,N)}, \boldsymbol{A}_{|U|\times|O|}\right)$, $v^* = \left(F^*_{L_0(M,N)}, \boldsymbol{A}^*_{|U|\times|O|}\right)$, $\boldsymbol{A}^*_{|U|\times|O|} = \|a^*_{uo}\|_{|U|\times|O|}$, регламентируемые функцией F_T и осуществляемые по конечному числу последовательных запросов вида $q \in Q$:

$$(\forall u \in U)(\forall o \in O | read \in a^*_{uo} \wedge read \in a_{uo}) \left(F^*_{L_0(M,N)}(u) \geq F^*_{L_0(M,N)}(o)\right); \quad (38)$$

$$(\forall u \in U)\begin{pmatrix}\forall o \in O | read \in a_{uo} \wedge \\ \wedge F^*_{L_0(M,N)}(u) < \\ < F^*_{L_0(M,N)}(o)\end{pmatrix}(read \notin a^*_{uo}); \quad (39)$$

$$(\forall u \in U)(\forall o \in O | write \in a^*_{uo} \wedge write \notin a_{uo}) \left(F^*_{L_0(M,N)}(u) \geq F^*_{L_0(M,N)}(o)\right); \quad (40)$$

$$(\forall u \in U)\begin{pmatrix}\forall o \in O | write \in a_{uo} \wedge \\ \wedge F^*_{L_0(M,N)}(u) < \\ < F^*_{L_0(M,N)}(o)\end{pmatrix}(write \notin a^*_{uo}). \quad (41)$$

Ограничения (38)-(41) используют понятие безопасности состояний (36) и (37).

Доказательство этой теоремы провели Белл и ЛаПадула, причём независимо от выбора используемой решётки уровней безопасности. Тем самым, в рассматриваемом в настоящей статье случае конечных нелинейных решёток основная теорема безопасности остается в силе.

ЗАКЛЮЧЕНИЕ

В представленном исследовании разработана такая математическая модель подсистемы обеспечения безопасности информации в АИС специального назначения, иерархически декомпозируемой по уровням безопасности, на основе которой удобно разрабатывать и анализировать сравнительно гибкие правила разграничения доступа к информации с высокой гарантированностью их выполнения за счёт использования математического аппарата конечных нелинейных решёток. Разработанная модель интегрирует принципы мандатного и дискреционного методов контроля доступа, рассматривая субъекты в роли посредников между пользователями и объектами. Высокая гарантированность защиты информации обеспечивается за счёт привлечения к анализу защищённости АИС специального назначения доказательной базы, присущей математическим моделям мандатной политики безопасности, в виде основной теоремы безопасности в модели Белла-ЛаПадулы, адаптированной подходящим образом к формализации уровней безопасности конечными нелинейными решётками.

СПИСОК ЛИТЕРАТУРЫ

1. Моисеев В.С., Дятчин В.В., Козар А.Н., Бутузова А.В. Об автоматизированных системах специального назначения // Исследования по информатике. – 2007. – Вып. 11. – С. 153–162.
2. Губин И.А., Губина С.С., Дубровин А.С., Сумин В.И. Описание политики безопасности эталонной модели защищенной автоматизированной системы // Вестник Тамбовского университета. Серия: Естественные и технические науки. – 2015. – Т. 20, № 5. – С. 1117–1120.
3. Сумин В.И., Громов Ю.Ю., Тютюнник В.М. Оптимизация функционирования информационных систем специального назначения // Научно-техническая информация. Сер.2. – 2023. – № 5. – С. 7–12. DOI: 10.36535/0548-0027-2023-05-1; Sumin V.I., Gromov Yu.Yu., Tyutyunnik V.M. Prospects for the Application of Digital Twin Systems and the Intellectualization of Calculations for the Strength of Chemical Equipment // Automatic Documentation and Mathematical Linguistics. – 2023. – Vol. 57, № 3. – P. 135–139.
4. Быковский А.Н., Дубровин А.С., Сумин В.И. Математическая модель политики безопасности подсистемы учёта труда и заработной платы защищенного информационного процесса финансовой деятельности // Вестник Воронежского государственного технического университета. – 2011. – Т. 7, № 9. – С. 38–40.
5. Дубровин А.С., Сумин В.И. Математическая модель политики информационной безопасности подсистемы эталонной автоматизированной системы обработки данных на основе ЭМЗАС-сети // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. – 2009. – № 1(56). – С. 26–44.
6. Заряев А.В., Сумин В.И., Застрожнов И.И., Дубровин А.С., Рогозин Е.А. Методическое обеспечение управления доступом пользователей к рабочей среде автоматизированных систем // Телекоммуникации. – 2004. – № 2. – С. 39–44.
7. Гретцер Г. Общая теория решёток / пер. с англ. А.Д. Больбота, В.А. Горбунова и В.И. Туманова; под ред. Д.М. Смирнова. – Москва: Мир, 1981. – 456 с.
8. Гайдамакин Н.А. Теоретические основы компьютерной безопасности : учебное пособие. – Екатеринбург: УрГУ, 2008. – 201 с.
9. Колмогоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа. – 7-е изд. – Москва: Физматлит, 2004. – 572 с.
10. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности: учеб. пособие для вузов. – Москва: Радио и связь, 2000. – 192 с.
11. Тютюнник В.М., Баканов А.С. Подходы к анализу информационных процессов в организации // Информационные ресурсы России. – 2023. – №2(191). – С. 58–71. DOI: 10.52605/16059921_2023_ 02_58.
12. Сумин В.И., Грачев Е.Д., Громов Ю.Ю., Тютюнник В.М. Математические модели определения времени обработки запросов на серверах информационных систем специального назначения // Научно-техническая информация. Сер. 2. – 2023. – № 10. – С. 11–15. DOI: 10.36535/0548-0027-2023-10-2; Sumin V.I., Grachev E.D., Gromov Yu.Yu., Tyutyunnik V.M. Mathematical Models for Determining the Time of Processing Requests on Servers of Special-Purpose Information Systems // Automatic Documentation and Mathematical Linguistics. – 2023. – Vol. 57, № 5. – P. 296–300.

Материал поступил в редакцию 27.10.24.

Сведения об авторах

ДУБРОВИН Анатолий Станиславович – доктор технических наук, доцент, профессор кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России
e-mail: Ibtks_kafedra@mail.ru

СУМИН Виктор Иванович – доктор технических наук, профессор, профессор кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России
e-mail: viktorsumin51@yandex.ru

ГРОМОВ Юрий Юрьевич – доктор технических наук, профессор, директор института автоматики и информационных технологий Тамбовского государственного технического университета (ТГТУ), профессор кафедры «Информационные системы и защита информации»
e-mail: gromovtambov@yandex.ru

ТЮТЮННИК Вячеслав Михайлович – доктор технических наук, профессор, профессор кафедры «Конструирование радиоэлектронных и микропроцессорных систем» ТГТУ, профессор кафедры библиотечно-информационных наук Московского государственного института культуры
e-mail: vmtyutyunnik@gmail.com