УДК 004.054.53 DOI:10.26102/2310-6018/2020.28.1.001

Методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления информационной безопасностью

В.В. Селифанов[1], Р.В. Мещеряков[2]
[1]Сибирский государственный университет геосистем и технологий, Новосибирск, Российская Федерация
[2]Институт проблем управления им. В.А. Трапезникова Российской академии наук, Москва, Российская Федерация

Резюме: Для обеспечения комплексной защиты информации необходимо использовать различные средства защиты информации, распределенные по уровням и сегментам информационной системы. Это создает противоречие, заключающееся в наличии большого количества различных средств защиты информации и невозможностью обеспечения их совместного согласованного применения при обеспечении защиты информации из-за отсутствия системы управления. Одной из задач, способствующих решению данной проблемы, является задача формирования допустимых вариантов организационного состава и структуры такой автоматизированной системы управления, результаты решения которой позволили бы получить такие варианты и выбрать из них оптимальный при заданных исходных параметрах и ограничениях. Задача решается сведением общей задачи к частной задаче разбиения на подграфы исходного графа автоматизированной системы управления кибербезопасностью. В таком случае подграфы будут соответствовать подсистемам автоматизированной системы управления на разных уровнях и обеспечат наглядное представление процесса формирования допустимых вариантов организационного состава и структуры такой автоматизированной системы управления. В результате выполнения операции разбиения графа на подзадачи будет получено множество допустимых вариантов организационного состава и структур автоматизированной системы управления кибербезопасностью, на основе которой осуществляется выбор оптимального при заданных исходных параметрах и ограничениях. Таким обрзом, сформирована методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления кибербезопасностью.

Ключевые слова: информационная безопасность, кибербезопасность, система защиты информации, управление, автоматизированная система управления.

Для цитирования: Селифанов В.В., Мещеряков Р.В. Методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления информационной безопасностью. *Моделирование, оптимизация и информационные технологии*. 2020;8(1). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/02/SelifanovMeshcherykov_1_20_1.pdf DOI:10.26102/2310-6018/2020.28.1.001

Methods of acceptable options formation of organizational structure and the structure of the automated information security management system

V.V. Selifanov[1], R.V. Meshcherykov [2]
[1]Siberian State University of Geosystems and Technology, Novosibirsk, Russian Federation
[2]V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russian Federation

Abstract. To ensure comprehensive information protection, it is necessary to use various means of information protection, distributed by levels and segments of the information system. This creates a contradiction, which consists in the presence of a large number of different means of information protection and the inability to ensure their joint coordinated application in ensuring the protection of information due to the lack of an automated control system. One of the tasks that contribute to the solution of this problem is the task of generating a feasible organizational structure and the structure of such an automated control system, whose results would provide these options and choose the one that is optimal under given initial parameters and limitations.The problem is solved by reducing the General problem to a particular problem of splitting into subgraphs of the original graph of the automated cyber defense control system. In this case, the subgraphs will correspond to the subsystems of the automated cyber defense management system at different levels and will provide a visual representation of the process of acceptable variants formation of the organizational composition and structure of such an automated control system. As a result of the operation of splitting into subtasks of the graph, a set of acceptable variants of the organizational composition and structures of the automated cyber defense management system are supposed to be obtained, based on which the optimal choice is made under the given initial parameters and restrictions. As a result, the technique of formation of admissible variants of organizational structure and structure by the automated control system of cyber defense is received.

Keywords: information security, cybersecurity, information protection, control, automated control systems.

For citation: SelifanovV.V., Meshcherykov R.V. Methods of formation of acceptable variants of organizational structure and structure of the automated information security management system. *Modeling, optimization and information technology*. 2020;8(1). Available by: https://moit.vivt.ru/wp-content/uploads/2020/02/SelifanovMeshcherykov_1_20_1.pdf DOI:10.26102/2310-6018/2020.28.1.001(In Russ.).

Введение

С вступлением в силу Федерального закона № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [1] большое внимание начало уделяться построению систем обеспечения безопасности значимых объектов критической информационной инфраструктуры (далее – ЗО КИИ).

Согласно [2] системы обеспечения безопасности ЗО КИИ имеют сложную многоуровневую структуру, представляющую собой совокупность средств защиты информации, используемых подразделениями (органами) защиты информации (далее – ЗИ) ЗОКИИ, организованную и функционирующую по установленным правилам и нормам [3-5],реализующую 27 групп мер, каждая из которых включает в себя функции автоматизированного управления [6].

В состав системы ЗИ должны быть включены разнородные силы и средства, которые могут быть распределены по достаточно большой территории (от объектового до федерального уровня, в том числе и при взаимодействии с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации), и обеспечено централизованное управление ими, а также оперативное распределение имеющегося ограниченного ресурса сил и средств ЗИ для обеспечения решения множества задач ЗИ одновременно или последовательно во времени. Основной проблемой при их использовании является противоречие, заключающееся в наличии большого количества различных средства защиты информации и невозможностью обеспечения их совместного согласованного применения при обеспечении защиты информации из-за отсутствия системы управления.

В данной ситуации одной из задач, способствующей решению данной проблемы является задача формирования допустимых вариантов организационного состава и структуры такой автоматизированной системы управления, результаты решения которой

позволили бы получить такие варианты и выбрать из них оптимальный при заданных исходных параметрах и ограничениях.

Наиболее правильным решением, в рассматриваемом случае, является выполнение функций управления в отдельной подсистеме, которая должна создаваться как автоматизированная адаптивная система оперативного управления [7-11] состав, структура и функции пунктов управления которой могут изменяться в зависимости от решаемых задач ЗИ.

Создание такой системы невозможно без формирования вариантов организационного состава и структуры автоматизированной системы управления кибербезопасности, где на первое место выходит научно-практическая задача формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления (далее – АСУ) кибербезопасностью.

Рассматриваемый вид АСУ представляет собой сложную систему и имеет различные состав и структуру, обеспечивающие реализацию всей совокупности возлагаемых на нее функций.

На первом этапе решения сформулированной задачи необходимо сформировать допустимые варианты организационного состава и структуры такой АСУ, из которых впоследствии можно было бы выбрать наилучший (оптимальный или субоптимальный) при заданных исходных данных и установленных ограничениях.

Стоит отметить, что в исследованиях, проводимых в последнее время [8-11, 13] приоритет отдается непосредственно механизмам обеспечения безопасности, при этом процесс управления считается заданным, а задача синтеза эффективных алгоритмов управления, как можно сделать вывод из [13], не ставится и не решается.

Задачей настоящего исследования является разработка методики формирования допустимых вариантов организационного состава и структуры АСУ кибербезопасностью.

Материалы и методы

К средствам защиты информации, в данной работе будем относить все элементы ЗО КИИ, реализующие функции безопасности, например, аутентификация, идентификация, регистрация событий и другие.

Под системой защиты информации будем понимать совокупность органов (подразделений и/или исполнителей), используемой ими средств защиты информации, функционирующих под управлением автоматизированной системы, а также объектов защиты информации, организованную и функционирующую по установленным правилам, нормам и политикам.

Под организационным составом и структурой автоматизированной системы управления будем понимать совокупность пунктов управления, связанных между собой отношениями подчиненности постоянно и/или временно.

Допустимыми вариантами организационного состава и структуры автоматизированной системы управления безопасностью будем считать варианты, удовлетворяющие принятым ограничениям и допущениям.

Задача формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления кибербезопасностью является сложной задачей [2, 14], сложность которой возрастает по экспоненциальному закону в зависимости от количества управляемых объектов (далее – УО). Для решения этой задачи в общем виде невозможно построить алгоритм, который всегда дает точное (оптимальное) решение и время работы которого никогда не превышает наперед заданной полиномиальной оценки, поэтому будем искать частное (субоптимальное) решение.

Известные подходы [13-16] к решению аналогичных задач предусматривают разбиение множества однородных управляемых объектов на некоторые подмножества случайным образом до тех пор, пока не будет получена оптимальная в смысле некоторого выбранного критерия структура подмножеств, или же последовательную декомпозицию задачи, решаемой системой управления, с последующей постановкой в соответствие декомпозированной задаче организационной структуры системы управления до получения оптимального количества уровней иерархии.

Рассматриваемая же задача отличается тем, что автоматизированная система управления решает не одну задачу, а множество последовательно и параллельно возникающих задач [17]. С учетом этого наиболее близким можно считать первый из рассмотренных подходов, который, в исходном виде, не может быть использован для решения данной задачи из-за большого количества получающихся при случайном разбиении переборных вариантов организационного состава и структуры автоматизированной системы управления кибербезопасностью. Представляется целесообразным для уменьшения сложности задачи воспользоваться предварительным объединением УО в группы (классы) в соответствии с имеющимися общими свойствами.

Сущность методики заключается в сведении общей сложной задачи - формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления к частной задаче разбиения на подграфы исходного графа АСУ кибербезопасностью с учетом предварительно проведенного группирования управляемых объектов.

Разбиение на подграфы исходного графа и введение дополнительных вершин для каждого подграфа приводит к появлению более сложной древовидной структуры, имеющей промежуточные вершины, которые соответствуют новым промежуточным пунктам управления в структуре АСУ кибербезопасностью. Таким образом, путем разбиения исходного графа на подграфы и введения дополнительных вершин для каждого подграфа, могут быть смоделированы допустимые варианты организационного состава и структуры АСУ кибербезопасностью различной степени сложности.

Результаты

В качестве исходного графа автоматизированной системы управления используется граф древовидной двухуровневой структуры, соответствующий простейшему организационному составу и структуре АСУ кибербезопасности. Пункт управления верхнего уровня непосредственно управляет всеми управляемыми объектами (Рисунок 1).

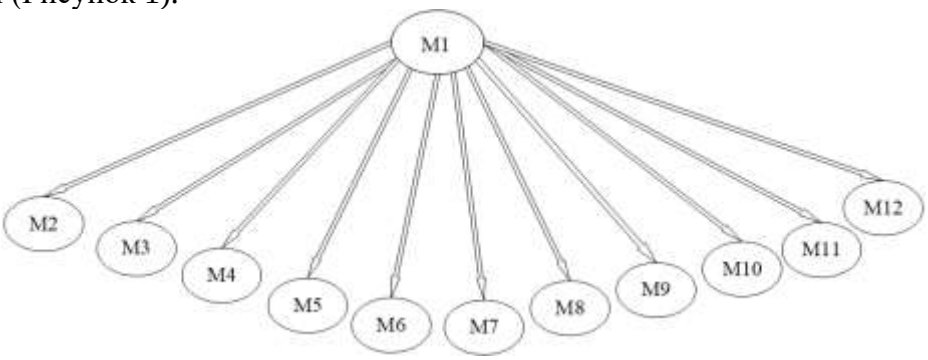

Рисунок 1 – Граф исходного простейшего организационного состава и структуры АСУ кибербезопасностью

Figure 1 – The graph of the initial simple organizational structure and structure of cyber security ACS

Вершины графа M_iна Рисунке 1 представляют собой пункты управления верхнего и нижнего уровня. Исходная автоматизированная система управления задана графом $G_M^{ИСУ}$ со множеством вершин

$$M = \{M_i\}, i = \overline{1, I} \quad (1)$$

набором рёбер

$$U = \{U_j\}, \ j = \overline{1, J} \quad (2)$$

и матрицей инциденций$\{b_{ij}\}$.

Совокупность управляемых объектов обладает признаками

$$l = \overline{1, L} \quad (3)$$

в соответствии с которыми они могут быть объединены в L групп УО, при этом каждый управляемый объект может входить только в одну группу.

Для ограничения числа рассматриваемых альтернативных вариантов состава и структуры АСУ кибербезопасностью задается максимальное число уровней управления и норма управляемости (количество подчиненных УО) для пунктов управления:

$$d_1 \le M_k \le d_2 \quad (4)$$

где d_1, d_2–значения показателей, определяемые нормой управляемости [13].

В качестве примеров подобного решения для защиты различных систем большое количество, в том числе и для значимых объектов КИИ, можно привести систему управления средствами защиты от несанкционированного доступа (Рисунок 2), построенную на базе семейства продуктов DallasLock [18].

Данное решение позволяет осуществлять управление кибербезопасностью небольших систем или сегментов крупных сетей.

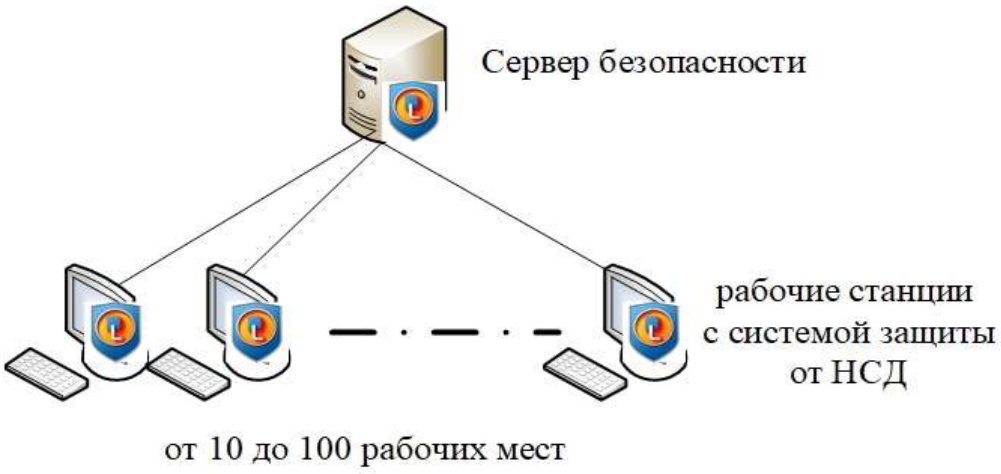

Рисунок2 –ПримердвухуровневойструктурыАСУкибербезопасностью, набазесемействапродуктовDallasLock

Figure 2 – An example of a two-tier cybersecurity ACS structure based on the Dallas Lock product family

Максимальная иерархическая организационная структура АСУ кибербезопасностью определяется использованием для управления пунктов управления всех существующих и планируемых к созданию уровней управления.

Вариант организационного состава и структуры АСУ кибербезопасностью максимальной сложности, соответствующий максимальному числу уровней управления n_{max}=6, а также норме управляемости d_1=2 и d_2=12, представлен на Рисунок 3.

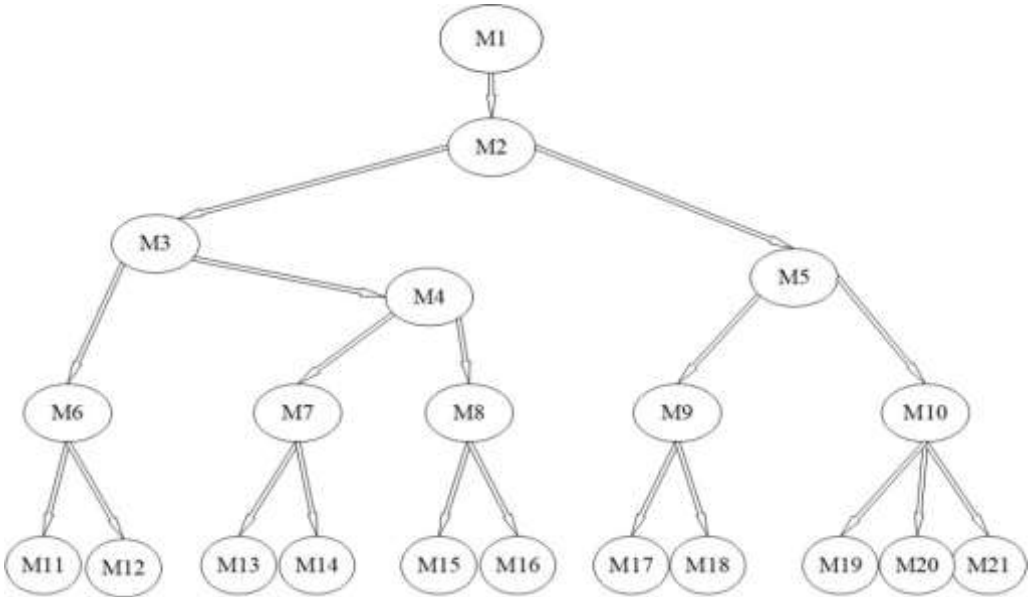

Рисунок 3 – Граф максимального организационного состава и структуры АСУ кибербезопасностью

Figure 3 – The graph of the maximum organizational structure and structure of the cyber security ACS

В качестве примера построения шести уровневой системы управления кибербезопасностью можно привести систему управления центром обработки данных на базе семейства продуктов DallasLock (Рисунок 4):

- на первом уровне – центр управления структурой кибербезопасности (как на виртуальном уровне, так и на физическом);
- на втором уровне – центры управления виртуальной инфраструктурой VMwarevSphere;
- на третьем – гипервизоры ESXi;
- на четвертом – менеджер серверов безопасности позволяющий создать несколько доменов безопасности, для управления средствами защиты, устанавливаемыми на виртуальные машины и сервера;
- пятый и шестой уровень – представляют собой сервер безопасности и рабочие станции с установленными СЗИ, по приведенной выше двухуровневой структуре.

Группирование управляемых объектов в соответствии с имеющимися у них общими свойствами предлагается осуществить по признакам методом Бонгарда. В соответствии с этим методом рассматривается множество управляемых объектов (1) и множество признаков

$$\Pi = \{\pi_l\}, \quad (5)$$

присутствующих в описании *i*-го УО, где π_l единичный признак который может принимать двоичные значения (типа «есть-нет»).

Для определения принадлежности или непринадлежности любого УО к определенной группе объектов строится решающая функция или решающее правило (6)

$$\varphi\{\pi_1^2,....,\pi_L^I\} \quad (6)$$

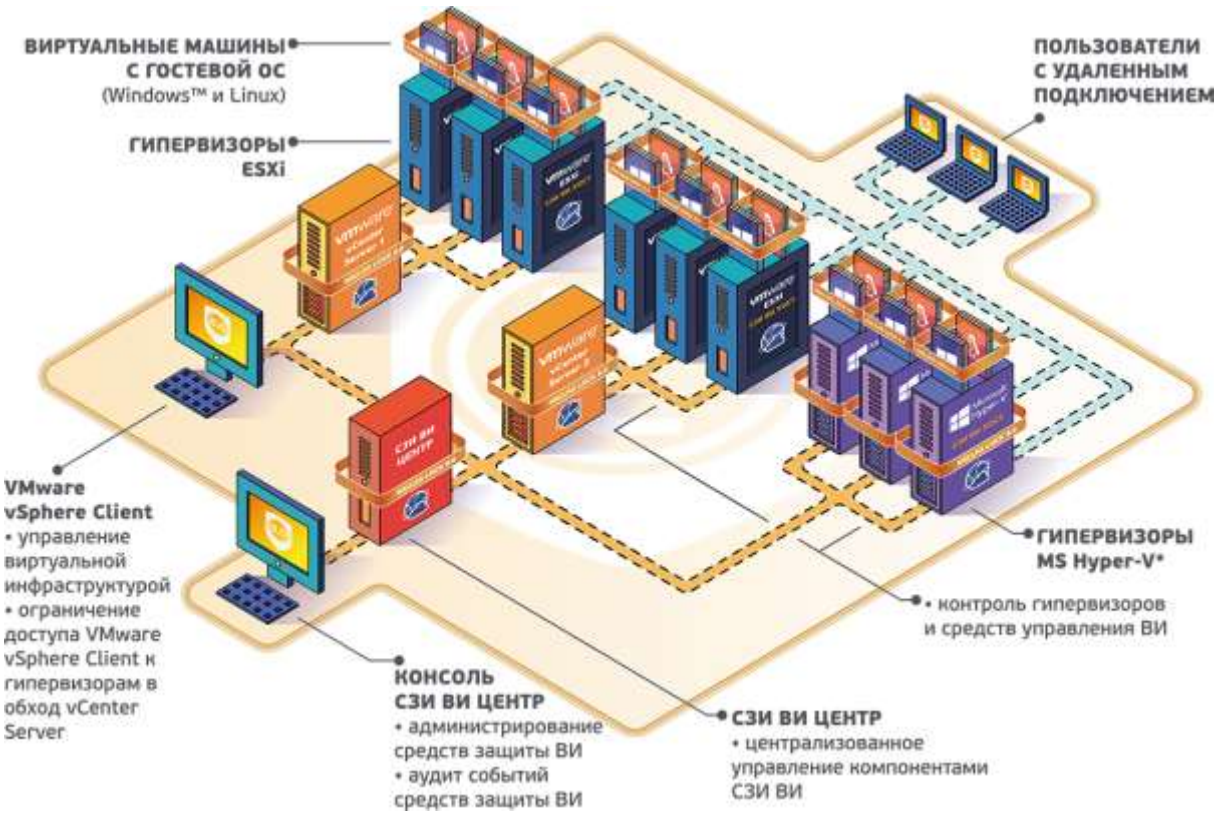

Рисунок 4 – Пример шестиуровневой структуры АСУ кибербезопасностью[19]
Figure 4 – An example of a six-level cyber security ACS structure [19]

Для рассматриваемого выше примера двух уровневой системы (Рисунок 2), в качестве признаков управления могут выступатьследующие признаки:

- уровни конфиденциальности (открытая и (или) конфиденциальная информация) обрабатываемой информации–l=1;
- наличие (отсутствие) подключения к сети Internet – l=2;
- возможность использования съемных машинных накопителей информации (USB-флэш накопителей) – l=3.

Для подобного случая L=3 и выражение (6) примет вид:

$$\varphi\{\pi_1^2,\pi_1^3,\pi_1^4,\pi_2^5,\pi_2^6,\pi_2^7,\pi_2^8,\pi_2^9,\pi_3^{10},\pi_3^{11},\pi_3^{12}\}. \quad (7)$$

Для обеспечения группирования для всех объектов, входящих в число объектов одной группы, решающая функция будет принимать значение равное единице хотя бы один раз и таким образом обеспечивается группирование УО в соответствии с имеющимися у них общими свойствами.

Для описания графа системы управления АСУ кибербезопасностью будем пользоваться матрицей инциденций, трансформировав ее классическое определение следующим образом: когда ребро U_j является петлей при вершине M_i будем считать b_{ij}=0. Получаемую таким образом матрицу инциденций графа G_M будем для краткости именовать по-прежнему матрицей инциденций и обозначать (8):

$$B(G_M) = \|b_{ij}\|, \tag{8}$$

где

$$b_{ij} = \begin{cases} 1 - если U_j \ ребро инцидентное вершине M_i \\ 0 - в других \quad случаях \end{cases}; \tag{9}$$

По определению матрицей разрезов графа G_M называется всякая матрица $R_{(GM)}$ строками которой являются векторы какой-либо базы пространства разрезов граф G_M. Матрицу разрезов можно получить путем преобразования матрицы инциденций за счет выполнения операций трех типов:

- перестановки столбцов;
- перестановки строк;
- замены строк.

Все эти три операции не меняют не только ранг матрицы, но и полную систему линейных зависимостей между ее столбцами – подсистема столбцов результирующей матрицы зависима или независима одновременно с подсистемой столбцов исходной матрицы.

Пользуясь этими операциями, можно преобразовать матрицу $B(G_M)$ к виду $B'(G_M)$, содержащему единичную подматрицу (10):

$$B'(G_M) = \begin{Vmatrix} 1 & 0 & \dots & 0 & b'_{1,p+1} & b'_{1,p+2} & \dots & b'_{1,m} \\ 0 & 1 & \dots & 1 & b'_{2,p+1} & b'_{2,p+2} & \dots & b'_{2,m} \\ . & . & . & . & . & . & . & . \\ 0 & 0 & \dots & 1 & b_{p,p+1} & b'_{p,p+2} & \dots & b'_{p,m} \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{Vmatrix}. \tag{10}$$

Удаляя из матрицы $B'(G_M)$ последние n-p строки, получим матрицу вида где (11):

$$\lambda = m - p, \tag{11}$$

где E_p^p - единичная матрица порядка p. Получившаяся матрица (12) является матрицей разрезов графа G_M, все строки которой, в соответствии с теорией графов [13], являются простыми разрезами.

$$R_m^p(G_M) = E_p^p B_\lambda^p \tag{12}$$

Объединяя простые разрезы в группы с учетом принадлежности соответствующих каждому разрезу УО группе с общими свойствами, получим блочно-диагональную матрицу разрезов.

Деление связного графа G_M по разрезу (13):

$$V_k \in R(G_M) \tag{13}$$

превращает G_M в два связных графа G_{M1} и G_{M2}, определяемых следующим образом. Обозначим через $G`_{M1}$ и $G`_{M2}$ компоненты суграфа (14)

$$G_M / V_k, \tag{14}$$

и положим (15)

$$G_{M1} = G'_{M1}V\{M_y\}, G_{M2} = G'_{M2}V\{M_y\}, \quad (15)$$

где M_y – новая вершина.

Отображение на ребрах V в графах $G`_{M1}$ и $G`_{M2}$ переопределим так, чтобы каждое ребро (16)

$$U_i \in V_k, \quad (16)$$

соединявшее в G_M вершину из $G`_{M1}$ с вершиной из $G`_{M2}$теперь соединяло в G_{M1} первую вершину с M_y, в G_{M2}это же ребро соединяло M_y со второй вершиной.

Деление графа $G_M^{ИСХ}$, описывающего исходную простейшую организационную структуру АСУ кибербезопасностью, осуществляется последовательно по всем группам разрезов, определяемым матрицей разрезов (17)

$$R_m^p(G_M^{ИСХ}), \quad (17)$$

в соответствии с проведенным ранее группированием УО. Выполнение операции деления и введения дополнительной вершины увеличивает на один количество уровней иерархии исходной структуры АСУ кибербезопасностью. Полученный в результате выполнения каждой операции деления исходного графа новый граф определяет возможный вариант организационного состава и структуры автоматизированной системы управлениякибербезопасностью.

Проверяя на соответствие введенным допущениям и ограничениям все полученные возможные варианты организационного состава и структуры и отбрасывая несоответствующие, получим множество допустимых вариантов.

Обсуждение

Последовательность действий при синтезе допустимых вариантов организационного состава и структуры АСУ кибербезопасностью будет следующей.

Шаг 1. Построение матрицы инциденций$B(G_M^{ИСХ})$ исходного графа $G_M^{ИСХ}$.

Шаг 2. Построение матрицы разрезов исходного графа (17).

Шаг 3. Группирование управляемых объектов в соответствии с их признаками.

Шаг 4. Разбиение управляемой системы в соответствии с максимальной нормой управляемости $M \le d_2$ и с учетом группирования управляемых объектов.

Шаг 5. Формирование матриц инциденций$B(G_M^{ДОП})$ сформированных вариантов организационного состава и структуры АСУ кибербезопасностью и их запоминание.

Шаг 6. Проверка достижения максимальной организационной структуры АСУ кибербезопасностью. Если не достигнута, то переход к шагу 3.

Шаг 7. По матрицам инциденций$B(G_M^{ДОП})$ сформированных вариантов строятся графы допустимых вариантов организационного состава и структуры автоматизированной системы управления $G_M^{ДОП}$.

Построением графов организационного состава и структуры автоматизированной системы управления завершается процедура синтеза допустимых вариантов организационного состава и структуры АСУ кибербезопасностью.

На Рисунках5 и 6 представлены примеры допустимых вариантов организационного состава и структуры АСУ кибербезопасностью.

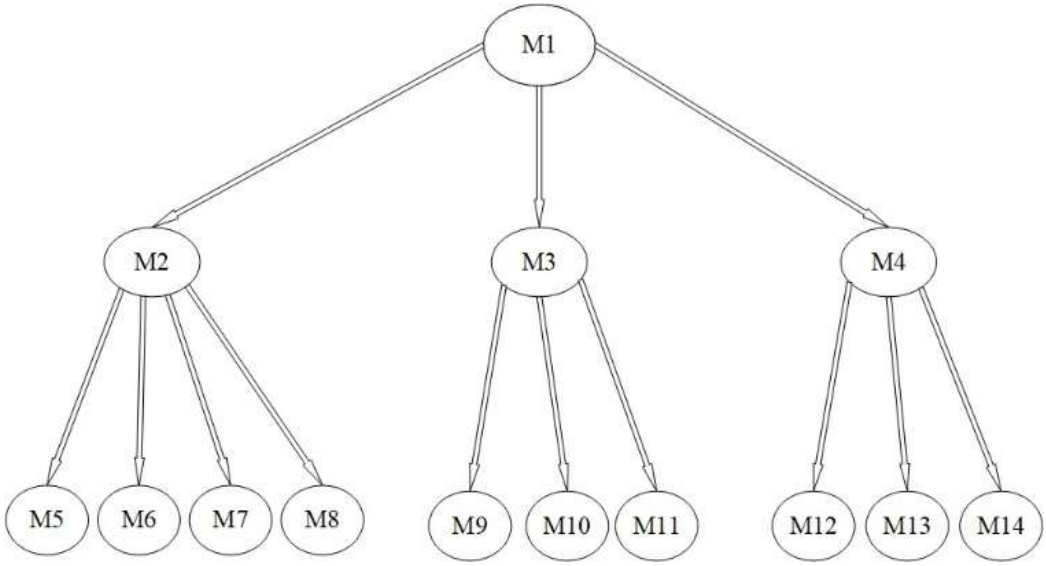

Рисунок 5 – Пример допустимого варианта трехуровневого организационного состава и структуры АСУ кибербезопасностью
Figure 5 – An example of an acceptable version of a three-level organizational structure and structure of cyber security ACS

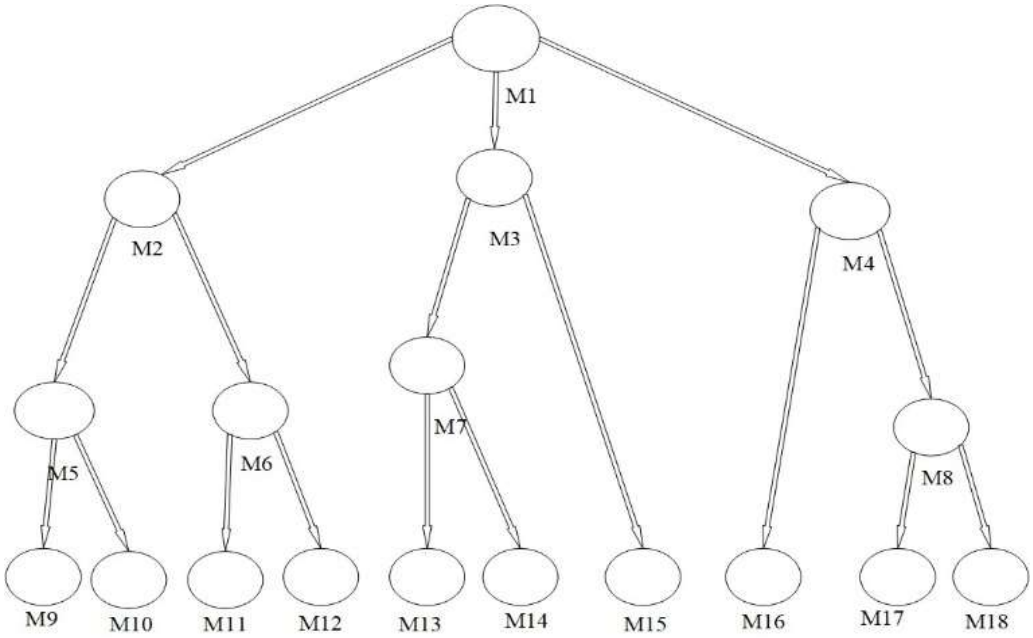

Рисунок 6 – Пример допустимого варианта четырехуровневого организационного состава и структуры АСУ кибербезопасностью
Figure 6 – An example of an acceptable variant of a four-level organizational structure and structure of cyber security ACS

Заключение

В результате выполнения операций разбиения на подграфы графа исходного организационного состава и структуры автоматизированной системы управления, будет получено множество допустимых вариантов организационного состава и структуры АСУ кибербезопасностью, из которых возможен выбор оптимального на основе проведения оценки эффективности.

В результате проведенных исследований разработана методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления кибербезопасностью применительно к значимым объектам информационной инфраструктуры. Сформированы допустимые варианты трех и четырехуровневого организационного состава, структуры автоматизированной системы управления кибербезопасностью, которые применялись авторами для построения различных систем управления защитой информации, а также их имитационных моделей [7, 12, 17].

ЛИТЕРАТУРА

1. Федеральный закон от 26.07.2017 №187 «О безопасности критической информационной инфраструктуры Российской Федерации»/ [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/acts/bank/42128, свободный (дата обращения: 15.05.2018).
2. Селифанов В.В. Методика формирования структуры функций управления защитой информации значимых объектов критической информационной инфраструктуры Российской Федерации. *Математические структуры и моделирование*. Омск. 2019; 1(49):97-106.
3. Methods for Testing & Specification; Risk-Based Security Assessment and Testing Methodologies, European Telecommunications Standards Institute, ETSI EG 201 015, 2015. [Online].https://www.etsi.org/deliver/etsi_eg/201000_201099/201015/02.01.01_60/eg_201015v020101p.pdf.
4. Cloud Flare. Zero-trust security: What’s a zero-trust network? 2019. [Online]. https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/.
5. Bellovin S. Layered Insecurity. *IEEE Security & Privacy*. 2019; 17(03): 96-95. DOI: 10.1109/MSEC.2019.2906807.
6. Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». [Электронный ресурс]. Режим доступа: https://minjust.consultant.ru/documents/38914, свободный (дата обращения: 15.05.2019).
7. ГолдобинаА.С., Исаева Ю.А. Выбор имитационной модели процессов управления защитой информации для оценки эффективности государственных и муниципальных систем. *Инновационное развитие науки и образования. Сборник статей Международной научно-практической конференции*. В 2 частях. Пенза. 2018:86.
8. Yener B., Gal T. Cybersecurity in the Era of Data Science: Examining New Adversarial Models. *IEEE Security & Privacy.* 2019;01:1-1,5555. DOI: 10.1109/MSEC.2019.2907097.
9. Peisert S. Control Systems Security from the Front Lines. *IEEE Security & Privacy*. 2014; 12(06):55-58. DOI: 10.1109/MSP.2014.105.
10. Choo K., Kermani M., Azarderakhsh R. and Govindarasu M. Emerging Embedded and Cyber Physical System Security Challenges and Innovations. *IEEE Transactions on Dependable and Secure Computing.* 2017; 14(03): 235-236. DOI: 10.1109/TDSC.2017.2664183.
11. Mailloux L., McEvilley M., Khou S. andPecarina J. Putting the «Systems» in Security Engineering: An Examination of NIST Special Publication 800-160.*IEEE Security & Privacy*. 2016; 14(04): 76-80. DOI: 10.1109 / MSP.2016.77.
12. Селифанов В.В., Голдобина А.С., Исаева Ю.А. Construction of Adapted Three-Level Model of Control Processes of Information Security System of Critical Information Infrastructure Objects. *Сборник трудов конференции «Актуальные проблемы*

электронного приборостроения АПЭП-2018. Proceedings XIV International scientific technical conference. In 8 Volumes. 2018».Новосибирск. 2018:148-153.
13. *Проблемы управления безопасностью сложных систем: материалы XXVI Междунар. конфер., 19 дек. 2018 г., Москва*; Под общ. ред. А.О. Калашникова, В.В. Кульбы. М.: ИПУ РАН. 2018:411.
14. Burkov V., Goubko M., Korgin N., Novikov D. Introduction to Theory of Control in Organizations. *New York: CRC Press*. 2015:352.
15. Novikov D., Chkhartishvili A. Reflexion and Control: Mathematical Models. *London: CRC Press*. 2014:298.
16. Novikov D. Theory of Control in Organizations. *New York: Nova Science Publishers*. 2013:341.
17. Селифанов В.В., Голдобина А.С., Исаева Ю.А., Климова А.М., Зенкин П.С. Построение адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры.*Доклады Томского государственного университета систем управления и радиоэлектроники*. Томск. 2018;21(4):51-58.
18. Конфидент. Централизованное и оперативное управление защищаемыми компьютерами в инфраструктурах любого размера и назначения. 2019. [Online]. https://www.dallaslock.ru/products/tsentralizovannoe-upravlenie/
19. Конфидент. Система защиты информации виртуальной инфраструктуры Dallas Lock // 2019. [Online]. https://www.dallaslock.ru/products/szvi-dallas-lock/

REFERENCES

1. Federal law No. 187 of 26.07.2017 *On security of critical information infrastructure of the Russian Federation*. [Electronic resource.] Mode of access: http://www.kremlin.ru/acts/bank/42128 free (date accessed: 15.05.2018).
2. Selifanov V.V. Methods of forming the structure of information protection management functions of significant objects of critical information infrastructure of the Russian Federation. *Mathematical structures and modeling*. Omsk. 2019;1(49):97-106.
3. Methods for Testing & Specification; Risk-Based Security Assessment and Testing Methodologies, European Telecommunications Standards Institute, ETSI EG 201 015, 2015.
[Online].https://www.etsi.org/deliver/etsi_eg/201000_201099/201015/02.01.01_60/eg_201015v020101p.pdf.
4. Cloud Flare. Zero-trust security: What's a zero-trust network? 2019. [Online]. https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/.
5. Bellovin S. Layered Insecurity. *IEEE Security & Privacy*. 2019;17(03):96-95. DOI: 10.1109/MSEC.2019.2906807.
6. Order of FSTEC of Russia dated 25.12.2017 No. 239 / *On approval of security Requirements for significant objects of critical information infrastructure of the Russian Federation*. [Electronic resource.] Mode of access: https://minjust.consultant.ru/documents/38914 free (date accessed: 15.05.2019).
7. Goldobina A.S., Isayeva J.A. The Choice of a simulation model of information protection management processes to assess the effectiveness of state and municipal systems. *Innovative development of science and education. Collection of articles of the International scientific-practical conference*. In 2 parts. Penza. 2018:86.
8. Yener B., Gal T. Cybersecurity in the Era of Data Science: Examining New Adversarial Models. *IEEE Security & Privacy*.2019;01:1-1,5555. DOI: 10.1109/MSEC.2019.2907097.
9. Peisert S. Control Systems Security from the Front Lines. *IEEE Security & Privacy*. 2014; 12(06):55-58. DOI: 10.1109/MSP.2014.105.

10. Choo K., Kermani M., Azarderakhsh R. and Govindarasu M. Emerging Embedded and Cyber Physical System Security Challenges and Innovations. *IEEE Transactions on Dependable and Secure Computing*. 2017; 14(03):235-236. DOI:10.1109/TDSC.2017.2664183.
11. Mailloux L., McEvilley M., Khou S. and Pecarina J. Putting the «Systems» in Security Engineering: An Examination of NIST Special Publication 800-160. *IEEE Security & Privacy*. 2016;14(04):76-80. DOI: 10.1109 / MSP.2016.77.
12. Selifanov V.V., Goldobina A.S., Isaeva J.A. Construction of Adapted Three-Level Model of Control Processes of Information Security System of Critical Information Infrastructure Objects. *Collection of the conference "Actual problems of electronic instrumentation APEP-2018. Proceedings of the XIV International scientific technical conference. In 8 Volumes. 2018"*. Novosibirsk. 2018: 148-153.
13. *Security management problems of complex systems: proceedings of XXVI international. confer., 19 Dec. 2018, Moscow*; Under the General editorship of A. O. Kalashnikov, V. V. Kul'by. M.: IPU Russian Academy of Sciences. 2018: 411.
14. Burkov V., Goubko M., Korgin N., Novikov D. Introduction to Theory of Control in Organizations. *New York: CRC Press*. 2015:352.
15. Novikov D., Chkhartishvili A. Reflexion and Control: Mathematical Models. *London: CRC Press*. 2014:298.
16. Novikov D. Theory of Control in Organizations. *New York: Nova Science Publishers.* 2013:341.
17. Selifanov V.V., Goldobina A.S., Isaeva J.A., Klimova A. M., Zenkin P.S. Construction of adaptive three-level model of management processes of information protection system of objects of critical information infrastructure. *Reports of Tomsk state University of control systems and Radioelectronics*. Tomsk. 2018; 21(4): 51-58.
18. Confidant. Centralized and operational management of protected computers in infrastructures of any size and purpose. 2019. [Online]. https: //www.dallaslock.ru/products/tsentralizovannoe-upravlenie/
19. Confidant. Virtual infrastructure information security system Dallas Lock // 2019. [Online]. https://www.dallaslock.ru/products/szvi-dallas-lock/

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATIONS ABOUT AUTHORS

Селифанов Валентин Валерьевич, доцент кафедры информационной безопасности, Сибирский государственный университет геосистем и технологий, Новосибирск, Российская Федерация.
e-mail: sfo1@mail.ru

Valentin V. Selifanov, Associate Professor of Information Security, Siberian state University of geosystems and technology, Novosibirsk, Russian Federation.

Мещеряков Роман Валерьевич, главный научный сотрудник, доктор технических наук, профессор Российской Академии Наук, Институт проблем управления им. В.А. Трапезникова Российской академии наук, , Российская Федерация.
e-mail: mrv@ipu.ru
ORCID: 0000-0002-1129-8434

Roman V. Meshcheryakov, Chief Researcher, Doctor of Technical Sciences, Professor of Russian Academy of Sciences, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russian Federation.