ISSN 1992-6502 (Print)
2020. Т. 24, № 1 (87). С. 76–84
Вестник УГАТУ
ISSN 2225-2789 (Online)
http://journal.ugatu.ac.ru

УДК 004.056

АНАЛИЗ ПРОСТРАНСТВЕННО-ВРЕМЕННОЙ МОДЕЛИ УГРОЗ ДЛЯ РАСПРЕДЕЛЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПРОЦЕССОМ ТРАНСПОРТИРОВКИ НЕФТЕГАЗОВОГО СЫРЬЯ

Т. В. Абрамова[1], **Т. З. Аралбаев**[2]

[1] t.v.abramova75@gmail.com, [2] atz1953@gmail.com

ФГБОУ ВО «Оренбургский государственный университет» (ОГУ)

Поступила в редакцию 25.02.2020

Аннотация. В статье предложен метод кластерного анализа пространственно-временной модели угроз для распределенной автоматизированной системы управления (АСУ) процессом транспортировки нефтегазового сырья. Описаны особенности построения модели угроз для распределенных управляющих систем и обоснована целесообразность применения кластерного анализа при ее исследовании. Предложена математическая модель кластеризации частных моделей угроз для подсистем распределенных АСУ, алгоритм и программное средство, реализующие данную модель. Проведен кластерный анализ частных моделей угроз для подсистем распределенной системы управления на примере АСУ процессом транспортировки нефтегазового сырья.

Ключевые слова: пространственно-временная модель угроз; кластерный анализ; распределенные АСУ; промышленные объекты нефтегазодобычи.

ВВЕДЕНИЕ

Одним из факторов эффективной защиты автоматизированных систем управления технологическим процессом (АСУ ТП) является построение адекватной модели угроз (МУ) информационной безопасности (ИБ). Построение МУ для распределенного объекта защиты сопряжено с такими сложностями, как разнообразный характер угроз антропогенного, техногенного и природного типа на различных его участках. В связи с этим значения рисков от угроз меняются для каждой из подсистем. Система защиты информации (СЗИ), построенная на основе общей модели угроз для всей АСУ, может быть адекватной для одних участков, но избыточной либо недостаточной для других. Это ведет к неэффективному использованию технических и временных ресурсов СЗИ.

Вопросы разработки и анализа моделей угроз для распределенных АСУ ТП рассматривались в работах [1–4]. Однако в доступной литературе недостаточно внимания уделено задаче построения и исследования моделей угроз для распределенных управляющих систем, в частности не рассматриваются вопросы систематизации и анализа МУ для подсистем распределенной АСУ ТП процессом транспортировки нефтегазового сырья. Тем не менее индивидуальный подход к разработке и исследованию МУ для каждой из подсистем АСУ позволит устранить избыточность СЗИ на одних участках и усилить защиту на других.

Целью работы является исследование частных моделей угроз для различных подсистем распределенных АСУ в условиях воздействия возмущений различного типа. Целью исследования является построение адекватной системы защиты информации на каждом участке АСУ на основе дифференцированного подхода, позволяющего снизить временные и стоимостные затраты на создание и модернизацию СЗИ.

Для достижения цели были решены следующие задачи:

– выявлены особенности построения модели угроз для распределенной управляющей системы транспортировки нефтегазового сырья;

– обоснована целесообразность применения кластерного анализа при исследовании пространственно-временной модели угроз;

– разработана математическая модель кластеризации частных моделей угроз для подсистем распределенных АСУ;

– разработан алгоритм и программное средство кластеризации частных моделей угроз для подсистем распределенных АСУ;

– проведен кластерный анализ частных моделей угроз для подсистем распределенной системы управления на примере АСУ процессом транспортировки нефтегазового сырья;

– предложены рекомендации для разработки модели угроз с учетом дифференцированного подхода.

ОСОБЕННОСТИ ПОСТРОЕНИЯ МОДЕЛИ УГРОЗ ДЛЯ РАСПРЕДЕЛЕННЫХ УПРАВЛЯЮЩИХ СИСТЕМ ТРАНСПОРТИРОВКИ НЕФТЕГАЗОВОГО СЫРЬЯ

Особенности топологического расположения распределенных АСУ ТП (протяженность в пространстве, удаленность компонентов АСУ от пунктов операторского и диспетчерского управления, рельеф местности, метеорологические условия) и различие факторов, влияющих на значения риска ИБ, обуславливают исследование угроз информационной безопасности для каждой из ее подсистем. Пример топологической схемы распределенной АСУ ТП транспортировки нефтегазового сырья приведен на рис. 1. Представленная АСУ разделена на подсистемы по функционально-топологическому принципу на этапе ее разработки. На рисунке оси координат ***NLat*** и ***ELong*** показывают координаты северной широты и восточной долготы соответственно, ***SubS1 – SubS10*** – исследуемые подсистемы АСУ.

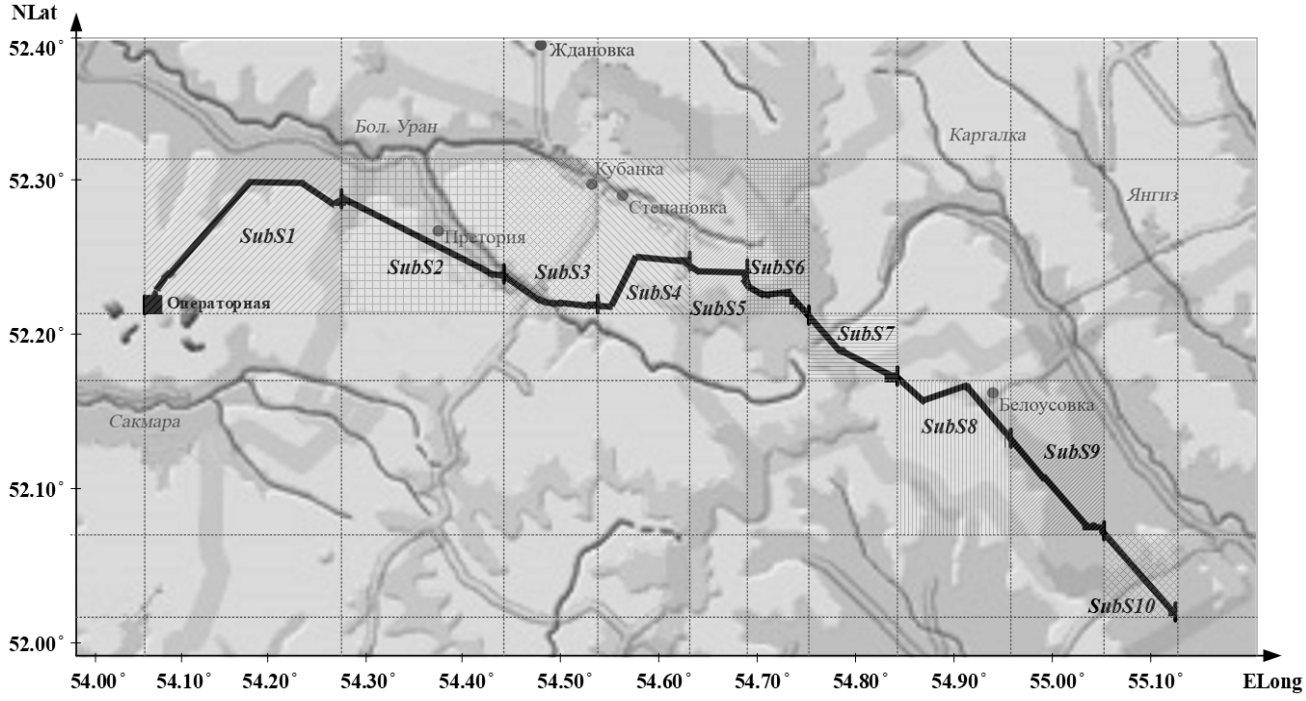


Рис. 1. Топологическая схема АСУ ТП транспортировки нефтегазового сырья

Исследование влияния угроз ИБ на каждую из подсистем АСУ показало переменный характер угроз на всей протяженности объекта. Это обусловлено влиянием техногенных и антропогенных угроз ввиду близкого расположения подсистем к дорогам и населенным пунктам, а также угроз природного типа, возникающих из-за особенностей рельефа (например, весенних паводков вблизи рек).

Наличие данных факторов создает необходимость дифференцированного подхода к построению системы защиты информации для распределенных АСУ ТП. Это предопределяет анализ пространственно-временной модели угроз (ПВМУ) в виде частных МУ и оценку рисков для каждой из подсистем.

ПРИМЕНЕНИЕ КЛАСТЕРНОГО АНАЛИЗА ПРИ ИССЛЕДОВАНИИ ПРОСТРАНСТВЕННО-ВРЕМЕННОЙ МОДЕЛИ УГРОЗ

Для решения задачи анализа ПВМУ целесообразно все множество частных МУ сгруппировать в кластеры по определенному признаку (например, по значению риска от угроз). Для решения задачи кластеризации частных МУ выбран метод k-средних, отличающийся оперативностью работы и простотой реализации.

При решении задачи исследования ПВМУ распределенных АСУ кластерный анализ позволяет:

– систематизировать множество частных моделей угроз;

– уменьшать вычислительную сложность задачи анализа большого числа частных МУ;

– выявлять группы подсистем с недостаточным либо избыточным уровнем защищенности в зависимости от условий их работы.

Риск информационной безопасности для i-й угрозы вычисляется по формуле (1):

$$R_i = P_i \cdot U_i, \qquad (1)$$

где P_i – вероятность реализации i-й угрозы; U_i – ущерб от реализации i-й угрозы.

При этом общее значение риска $R_{общ}$ для распределенной системы складывается из значений рисков от каждой угрозы для каждой из подсистем и вычисляется по формуле (2):

$$R_{общ} = \sum_{i=1}^{L} \sum_{j=1}^{N} R_{ij} \qquad (2)$$

$$T_{реал} \le T_{огр};\ Z_{реал} \le Z_{огр},$$

где R_{ij} – риск при реализации i-й угрозы для j-й подсистемы; L – число угроз информационной безопасности; N – общее число подсистем АСУ; $T_{реал}$ и $Z_{реал}$ – соответственно, реальное время обнаружения факта реализации угрозы и затраты на систему обнаружения; $T_{огр}$ и $Z_{огр}$ – временные и стоимостные ограничения для СЗИ.

Каждая j-я подсистема характеризуется особенностями ее эксплуатации, расположения ее узлов, их функционирования в течение года. Эти особенности напрямую влияют на содержание частных МУ каждой подсистемы. Пространственные координаты (x_j, y_j) определяют границы подсистем. Они влияют на вероятность реализации угроз, связанных с особенностями рельефа местности и расположением вблизи объекта автомобильных дорог, городов, поселков. Временные характеристики работы системы t определяют периодичность и сезонность проявления угроз.

Таким образом, при разработке и анализе ПВМУ ставится задача построения множества частных моделей угроз с учетом особенностей расположения и эксплуатации каждой из подсистем и объединения их в кластеры для дальнейшего анализа.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КЛАСТЕРИЗАЦИИ ЧАСТНЫХ МОДЕЛЕЙ УГРОЗ ДЛЯ ПОДСИСТЕМ РАСПРЕДЕЛЕННЫХ АСУ

Задача кластерного анализа частных МУ представляется следующим образом. Пусть дано:

– $M = \{M_1, M_2, ..., M_N\}$ – множество частных МУ, каждая из которых содержит конечный перечень угроз ИБ;

– N – общее число частных МУ для N подсистем;

– $U = \{U_1, U_2, ..., U_L\}$ – множество угроз ИБ;

– L – общее число угроз ИБ.

Задача кластерного анализа заключается в построении множества кластеров $C = \{C_1, C_2, ..., C_k, ... C_{N^*}\}$, содержащего N^* элементов. Каждый кластер включает перечень частных МУ из множества M. Значения рисков R_{ij} одних и тех же угроз близки для всех частных МУ, входящих в один кластер.

Математическое описание процедуры кластерного анализа ПВМУ представлено в выражениях (3)–(4).

$$K_n = k_{1n}, k_{2n}, \ldots, k_{ln}$$

$$k_{\ln} = \begin{cases} 1, \text{ если } R_{ln} \geq s_l; \\ 0, \text{ если } R_{ln} < s_l; \end{cases} \quad (3)$$

$$s_l = \frac{\sum_{n=1}^{N} R_{\ln}}{N}, \; l = 1, \text{L}, \quad (4)$$

где R_{ln} – значение риска l-й угрозы n-й модели; s_l – среднее значение риска. Число угроз L одинаково для каждой из частных МУ и определяется количеством угроз в модели угроз для АСУ.

В качестве параметра кластеризации в рамках работы приняты риски от угроз ИБ. Мера сходства между частными МУ определяется по классификационным кодам моделей, рассчитываемым на основе средних значений рисков s_l. Совокупный классификационный код K_n ($n = 1, N$) частной МУ представляет из себя ряд бинарных значений k_{nl}, каждое из которых определяется согласно выражениям (3)–(4).

При этом возможно проведение кластерного анализа по двум вариантам:

– кластерный анализ h-типа: классификационные коды формируются на основе средних значений рисков по каждой угрозе во всех частных МУ;

– кластерный анализ v-типа: классификационные коды формируются на основе средних значений рисков по всем угрозам для каждой частной МУ.

Таким образом, математическая модель кластеризации частных МУ может быть представлена в виде двумерной матрицы, изображенной на рис. 2. По строкам матрицы располагаются наименования угроз, по столбцам – идентификаторы частных МУ.

В каждую из ячеек таблицы заносятся бинарные значения k^h и k^v для построения классификационных кодов h-типа и v-типа соответственно. Параметр s_l вычисляется как среднее значение показателей k^h для каждой строки матрицы в случае кластеризации h-типа либо среднее значение показателей k^v для каждого столбца матрицы в случае кластеризации v-типа.

Частные МУ / Угрозы	$M1$	$M2$	…	M_N	Совокупный классификационный код h-типа
$U1$	$k^h_{1.1}$ / $k^v_{1.1}$	$k^h_{1.2}$ / $k^v_{1.2}$	…	$k^h_{1.N}$ / $k^v_{1.N}$	$k^h_{1.1}, k^h_{1.2}, \ldots, k^h_{1.N}$
$U2$	$k^h_{2.1}$ / $k^v_{2.1}$	$k^h_{2.2}$ / $k^v_{2.2}$	…	$k^h_{2.N}$ / $k^v_{2.N}$	$k^h_{2.1}, k^h_{2.2}, \ldots, k^h_{2.N}$
…	…	…	…	…	…
U_L	$k^h_{L.1}$ / $k^v_{L.1}$	$k^h_{L.2}$ / $k^v_{L.2}$	…	$k^h_{L.N}$ / $k^v_{L.N}$	$k^h_{L.1}, k^h_{L.2}, \ldots, k^h_{L.N}$
Совокупный классификационный код v-типа	$k^v_{1.1}, k^v_{2.1}, \ldots, k^v_{L.1}$	$k^v_{1.2}, k^v_{2.2}, \ldots, k^v_{L.2}$	…	$k^v_{1.N}, k^v_{2.N}, \ldots, k^v_{L.N}$	Совокупный классификационный код

Рис. 2. Матрица кластеризации

Данный подход позволил получить кластеры частных МУ с близкими характеристиками угроз по перечню и по величинам их рисков.

АЛГОРИТМ И ПРОГРАММНОЕ СРЕДСТВО КЛАСТЕРИЗАЦИИ ЧАСТНЫХ МОДЕЛЕЙ УГРОЗ ДЛЯ ПОДСИСТЕМ РАСПРЕДЕЛЕННЫХ АСУ

Представленная математическая модель была реализована в виде алгоритма, схема которого изображена на рис. 3.

В качестве исходных данных для работы алгоритма выступает множество частных моделей угроз. Частные МУ представлены в виде матриц, в строках которых содержатся порядковые номера угроз, а в столбцах – данные о наименовании угрозы и значении риска от угрозы. Для принятия решения об отнесении частной МУ к определенному кластеру производится расчет средних значений рисков для каждой из угроз по всем частным моделям и определение классификационных кодов по формулам (3)–(4).

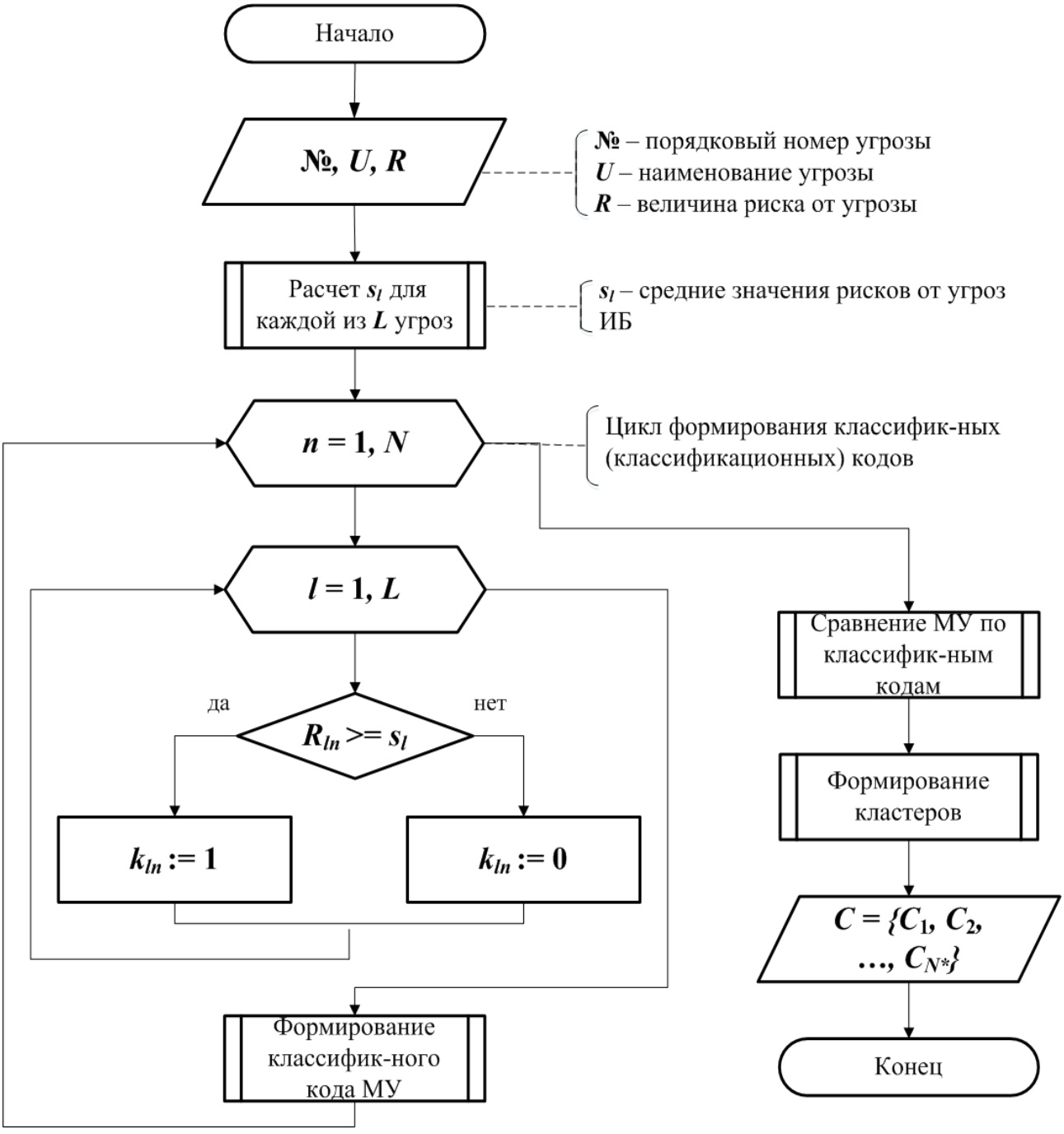


Рис. 3. Схема алгоритма кластеризации частных моделей угроз

В результате анализа исходное множество частных МУ, содержащее ***N*** элементов, объединяется в множество кластеров, содержащее ***N**** элементов. Каждый кластер включает частные МУ с близкими характеристиками угроз. Для подсистем, МУ которых входят в один кластер, применима общая модель угроз. В том случае, если в результате кластеризации получен один кластер, исследования угроз для всех участков объекта проводятся на основе одной МУ.

Разработанный алгоритм использован при исследовании модели угроз для АСУ ТП транспортировки нефтегазового сырья, представленной в работе [8]. Рассматриваемая АСУ на этапе ее проектирования была разбита по функциональным характеристикам на 10 подсистем, как показано на рис. 1. Для исследования модели угроз рассматриваемого объекта было разработано программное средство [9], реализующее предложенный алгоритм.

Экранная форма работы программы представлена на рис. 4. При построении частных МУ были выбраны актуальные угрозы, характерные для данной АСУ: ***A*** – атаки через корпоративную сеть передачи данных на традиционные IT-компоненты, применяемые в АСУ; ***B*** – несанкционированное использование технологий удаленного доступа; ***C*** – перехват, искажение и передача информации, циркулирующей в сети; ***D*** – нерегламентированные действия персонала; ***E*** – нарушение целостности линий связи.

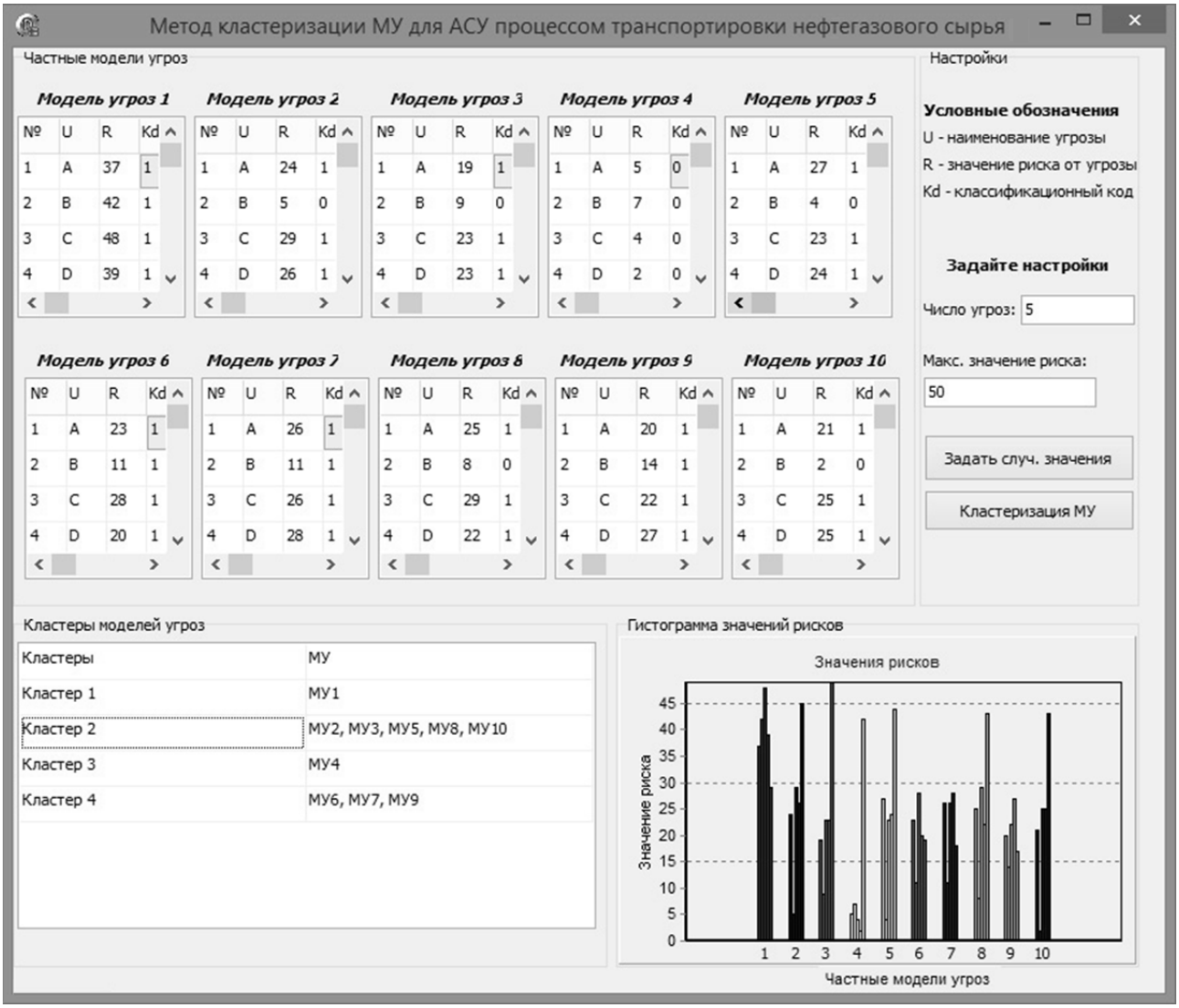


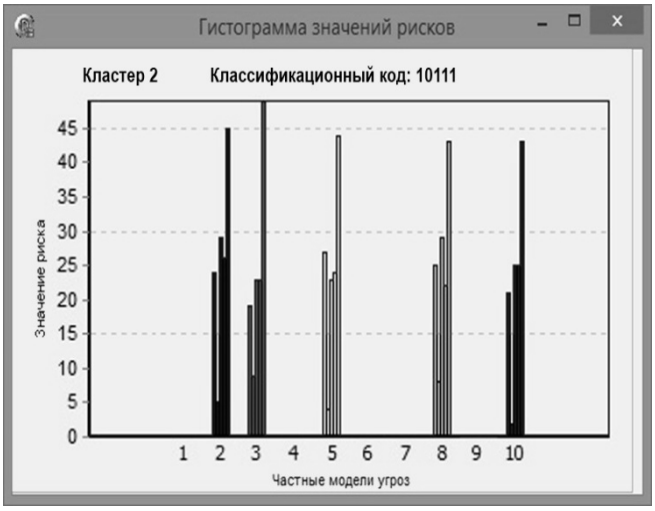
Рис. 4. Экранная форма работы программы «Метод кластеризации моделей угроз для распределенной АСУ процессом транспортировки нефтегазового сырья»

КЛАСТЕРНЫЙ АНАЛИЗ ЧАСТНЫХ МОДЕЛЕЙ УГРОЗ ДЛЯ ПОДСИСТЕМ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ НА ПРИМЕРЕ АСУ ПРОЦЕССОМ ТРАНСПОРТИРОВКИ НЕФТЕГАЗОВОГО СЫРЬЯ

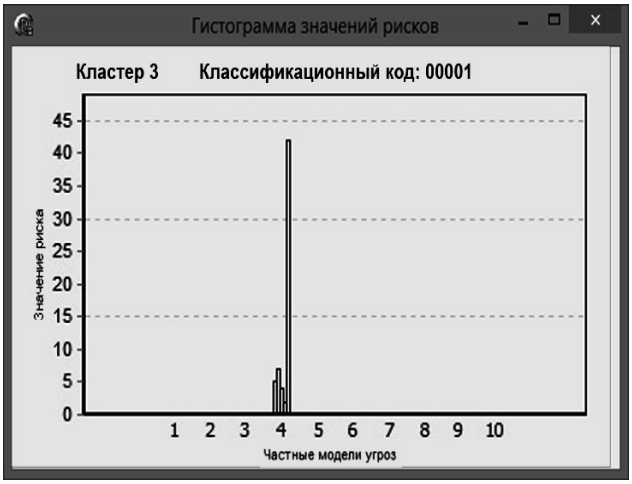
В результате анализа было получено 4 кластера частных МУ. На рис. 5 видно, что все частные МУ, входящие в один кластер, характеризуются близкими значениями рисков для одних и тех же угроз. Например, частные модели угроз для подсистем АСУ кластера 2 содержат высокие значения риска от угрозы нарушения целостности линии связи, так как соответствующие подсистемы находятся вблизи рек, дорог и населенных пунктов. Эти факторы создают опасность обрыва в результате размыва почв и прохождения тяжелой техники в районе прокладки кабеля. Угроза несанкционированного использования технологий удаленного доступа, напротив, невелика, так как расматриваемые подсистемы не содержат компонентов верхнего уровня управления.

Таким образом, для разработки и исследования модели угроз для рассматриваемой АСУ, состоящей из 10 подсистем, достаточно 4 частных МУ.

а



б



в

г

Рис. 5. Гистограммы значений рисков от угроз для частных МУ:
а – кластера 1; б – кластера 2; в – кластера 3; г – кластера 4

При исследовании временных особенностей проявления угроз условия работы каждой из подсистем АСУ рассматриваются в конкретный период времени. Например, при исследовании сезонного изменения величин рисков для подсистем АСУ строятся четыре группы частных МУ и каждая из групп кластеризуется и исследуется отдельно. Таким образом, полученные данные позволяют оценить значения рисков от угроз и выявить особенности влияния техногенных, антропогенных и природных факторов в течение года на каждую из подсистем.

Достоинствами представленного метода являются:

– простота и наглядность анализа ПВМУ распределенных систем управления;

– учет условий эксплуатации каждой из подсистем распределенной АСУ ТП;

– минимизация временных и финансовых затрат на создание и модернизацию СЗИ при сохранении основных требований по защите информации.

РЕКОМЕНДАЦИИ ДЛЯ РАЗРАБОТКИ МОДЕЛИ УГРОЗ С УЧЕТОМ ДИФФЕРЕНЦИРОВАННОГО ПОДХОДА

Разработанные модель и алгоритм кластерного анализа МУ могут быть использованы при обеспечении информационной безопасности не только стационарных, но и мобильных объектов информатизации, которые, перемещаясь в пространстве, подвергаются различным угрозам. В настоящее время подобные разработки ведутся для наземных и воздушных объектов мониторинга. В работах [5–7] рассмотрены вопросы построения и кластерного анализа моделей угроз для мобильных объектов мониторинга АСУ ТП. Полученные результаты рекомендуются для разработки систем защиты информации с учетом дифференцированного подхода.

ЗАКЛЮЧЕНИЕ

Представленный метод позволил систематизировать множество частных моделей угроз для подсистем АСУ ТП, выявить наиболее уязвимые компоненты АСУ и подсистемы с избыточной защитой. Дифференцированный подход к построению моделей угроз для распределенных управляющих систем позволил повысить эффективность СЗИ и уменьшить временные и стоимостные затраты на организацию системы защиты информации в АСУ.

СПИСОК ЛИТЕРАТУРЫ

1. **Базовая** модель угроз безопасности информации в ключевых системах информационной инфраструктуры [Электронный ресурс]. URL: https://zlonov.ru/laws/ics/ (дата обращения 10.11.2018). **[** (2018, Nov. 11). *The basic model of information security threats in key information infrastructure systems* [Online], (in Russian). Available: https://zlonov.ru/laws/ics/ **]**

2. **Типовая** модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена // Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. URL: https://zakonbase.ru/content/part/1183316 (дата обращения 02.11.2019). **[** (2019, Nov. 2). *A typical model of personal data security threats processed in distributed personal data information systems that do not have a connection to public communication networks and (or) international information exchange networks* // Basic model of personal data security threats when they are processed in personal data information systems [Online], (in Russian). Available: https://zakonbase.ru/content/part/1183316 **]**

3. **Попова А. Д., Богданов П. А., Быков Д. В.** Разработка автоматизированной системы моделирования угроз безопасности [Электронный ресурс]. URL: https://sibac.info/journal/student/27/103048 (дата обращения 03.11.2019). **[** A. D. Popova, P. A. Bogdanov and D. V. Bykov (2019, Nov. 3). *Development of an automated security threat modeling system* [Online], (in Russian). Available: https://sibac.info/journal/student/27/103048 **]**

4. **Классификация** методов защиты информации на основе кластерного анализа / В. В. Меньших и др. // Вестник ВГТУ. 2009. Т. 5, № 6. С. 203–205. **[** V. V. Menshih, et. al., “Classification of information protection methods based on cluster analysis”, (in Russian), in *Vestnik VGTU,* vol. 5, no. 6, pp. 203-205, 2009. **]**

5. **Аралбаев Т. З., Абрамова Т. В., Гетьман М. А.** Кластерный анализ как инструмент построения и исследования пространственно-временных моделей угроз // Университетский комплекс как региональный центр образования, науки и культуры: материалы Всероссийской научно-методической конференции. Оренбург: ОГУ, 2020. С. 1401–1405. **[** T. Z. Aralbaev, T. V. Abramova and M. A. Getman, “University complex as a regional center of education, science and culture”, in *All-Russian Scientific and Methodological Conference* (OSU 2020), 2020, pp. 1401-1405. **]**

6. **Getman M., Aralbaev T.** Method of coding and classification of information security threats for mobile objects based on matrix model // Polish journal of science. 2019. Vol. 1, no. 22. Pp. 43-46. **[** M. Getman and T. Aralbaev, “Method of coding and classification of information security threats for mobile objects based on matrix model”, (in Russian), in *Polish journal of science,* vol. 1, no 22, pp. 43-46, 2019. **]**

7. **Аралбаев Т. З., Гетьман М. А.** Прикладная программа «Кластерный анализ моделей угроз для мобильных объектов информатизации» [Электронный ресурс]. URL: https://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&action=details&ufer_id=2023 (дата обращения 08.02.2020). **[** T. Z. Aralbaev and M. A. Getman (2020, Feb. 8). *Application program "Cluster analysis of threat models for mobile informatization objects"* [Online]. Available: https://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&action=details&ufer_id=2023 **]**

8. **Оптимизация** методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков: монография / Т. З. Аралбаев и др. Оренбург: ОГУ, 2018. 160 с. **[** T. Z. Aralbaev, et. al., *Optimization of methods for monitoring the technical condition of distributed automated systems under the influence of spatio-temporal threats based on monitoring of network information flows,* (in Russian). Orenburg: OGU, 2018. **]**

9. **Абрамова Т. В., Аралбаев Т. З.** Прикладная программа «Метод кластеризации моделей угроз для распределенной АСУ процессом транспортировки нефтегазового сырья» [Электронный ресурс]. URL: https://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&actIon =details&ufer_id=2022 (дата обращения 08.02.2020). **[** T. V. Abramova and T. Z. Aralbaev (2020, Feb. 8). *Application program "Cluster method of threat models for distributed ACS by the process of transportation of oil and gas raw materials"* [Online]. Available: https://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&action=details&ufer_id =2022 **]**

ОБ АВТОРАХ

АБРАМОВА Таисия Вячеславовна, асп. каф. ВТиЗИ ФГБОУ ВО «ОГУ». Дипл. «Информационная безопасность» (ОГУ, 2015). Дипл. «Информатика и вычислительная техника» (ОГУ, 2017). Готовит дис. на тему «Обнаружение и нейтрализация аномалий в распределенных автоматизированных системах транспортировки нефтегазового сырья на основе мониторинга сетевых информационных потоков».

АРАЛБАЕВ Ташбулат Захарович, проф. каф. ВТиЗИ ФГБОУ ВО «ОГУ». Дипл. инженер-электрик (1975). Д-р техн. наук по автоматизации и управлению технологическими процессами и производствами (ОГУ, 2004). Иссл. в обл. контроля и диагностики вычислительных и инфокоммуникационных систем и сетей.

METADATA

Title: Analysis of a space-temporary threat model for a distributed automated system of management of the process of transportation of oil and gas raw materials.

Authors: T. V. Abramova[1], T. Z. Aralbaev[2]

Affiliation:

Orenburg State University (OSU), Russia.

Email: [1]t.v.abramova75@gmail.com, [2]atz1953@gmail.com

Language: Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), vol. 24, no. 1 (87), pp. 76-84, 2020. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: The article proposes a method of cluster analysis of the spatio-temporal threat model for a distributed automated control system (ACS) for the transportation of oil and gas raw materials. The features of building a threat model for a distributed control system are described and the feasibility of using cluster analysis in its study is justified. A mathematical model is proposed for clustering private threat models for distributed ACS subsystems, an algorithm and software that implement this model. A cluster analysis of private threat models for subsystems of a distributed control system is carried out on the example of an automated control system for the transportation of oil and gas raw materials.

Key words: spatio-temporal threat model; cluster analysis; distributed ACS; industrial oil and gas production facilities.

About authors:

ABRAMOVA, Taisia Vyacheslavovna, Postgrad. (PhD) Student Dept. of Computing and Information Security (OSU). Bachelor of Information Security (OSU, 2015). Master in Computer Science and Computer Engineering (OSU, 2017).

ARALBAEV, Tashbulat Zakharovich, prof. Dept. of Computing and Information Security (OSU). Dipl. Electrical Engineer (1975). Dr. of Tech. Sci. (OSU, 2004).