3. De Lucia M.J., Cotton C. Identifying and detecting applications within TLS traffic. *Proceedings Cyber Sensing*, 2018, vol. 10630, pp. 106300U.
4. Sheluhin O.I., Sakalema D.Zh., Filinova A.S. *Detection of Intrusions into Computer Networks (Network Anomalies): Textbook for Universities*. Moscow: Goryachaya liniya – Telekom, 2022, 220 p. (In Russ.)
5. Sharma S., Krishna C.R., Sahay S.K. Detection of advanced malware by machine learning techniques. *Springer, Advances in Intelligent Systems and Computing*, 2018, vol. 742, pp. 332–342.
6. CSE-CIC-IDS2018 on AWS. URL: http://www.unb.ca/cic/datasets/ids-2018.html (accessed: 18.12.2023).
7. Intrusion Detection Evaluation Dataset (CIC-IDS2017). URL: https://www.unb.ca/cic/datasets/ids-2017.html (accessed: 18.12.2023).
8. Ferriyan A. et al. HIKARI-2021: Generating network intrusion detection dataset based on real and encrypted synthetic attack traffic. URL: https://zenodo.org/records/5199540 (accessed: 20.01.20244).
9. Catillo M. et al. USB-IDS-1: A public multilayer dataset of labeled network flows for IDS evaluation. *51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops* (DSN-W), 2021, pp. 1–6. DOI: 10.1109/DSN-W52860.2021.00012
10. Harrison M. *Machine Learning: A Pocket Guide. A Quick Guide to Structured Machine Learning Methods in Python*. Transl. from English by V.A. Kovalenko. Saint Petersburg: Dialektika, 2020, 320 p. (In Russ.)

*Received 22.01.2024*

## ТЕХНОЛОГИИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

УДК 004.056

# МОДЕЛИ И АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ НА ОСНОВЕ ЭКСПЕРТНОГО ПОДХОДА

*Рычкова А.А.[1], Долгушев Н.А.[1,3], Бурькова Е.В.[1], Коннов А.Л.[1,2]*
*[1] Оренбургский государственный университет, Оренбург, РФ,*
*[2] Оренбургский филиал Поволжского государственного университета телекоммуникаций и информатики, Оренбург, РФ,*
*[3] Оренбургский филиал ООО «Уральский центр систем безопасности», Оренбург, РФ*
*E-mail: rnansy@yandex.ru, dolgushevn1@yandex.ru, tulpan63@bk.ru, andrey_konnov@mail.ru*

Задача определения актуальных угроз безопасности приобретает все большее значение, что обусловлено ростом объемов обрабатываемой информации ограниченного доступа, увеличением количества всевозможных угроз, повышением потенциала нарушителей. На предприятиях и в организациях разных сфер экономики специалисты регулярно проводят аудит информационной безопасности с целью выявления уязвимостей и в конечном итоге для предотвращения возможных негативных последствий. Для построения рациональной системы безопасности информации на объекте важно организовать защиту именно от актуальных угроз, так как от всех угроз построить защиту невозможно, да и нецелесообразно. В статье предложены модели и алгоритмы определения актуальных угроз на основе экспертного подхода, которые могут стать базисом для разработки автоматизированной системы принятия достоверных решений в задачах защиты объектов информатизации.

***Ключевые слова:*** *угроза безопасности, метод анализа иерархий, иерархическая модель*

### Введение

Для определения актуальных угроз используют различные методы [2; 3; 7; 9], учитывают особенности для конкретных сфер деятельности [5], существуют также автоматизированные системы на основе программных продуктов [12]. Все эти методы основаны на положениях методики оценки угроз безопасности федеральной службы по техническому и экспортному контролю (ФСТЭК) России от 2021 года. Учитывается необходимость проведения основных этапов этого процесса: анализа защищаемых объектов, определения не-

гативных последствий, характеристики нарушителя, составления сценариев реализации угроз.

## Предлагаемые модели и алгоритмы

Модель угроз разрабатывается группой экспертов, у которых есть опыт в сфере информационной безопасности, есть доступ к аппаратным и программным средствам информационных систем предприятия, доступ к активам, для осуществления оценки как ценности защищаемых ресурсов, так и уровня защищенности их на данном объекте. Эксперт при разработке модели угроз основывается на объективных данных, таких как требования и положения нормативно-правовых документов ФСТЭК России, проведенном аудите инфраструктуры предприятия, сведении об актуальных уязвимостях в системном и прикладном программном обеспечении. В роли экспертов могут выступать сотрудники организации с соответствующей квалификацией в области информационной безопасности или сторонние специалисты. В первом случае эксперты хорошо знакомы с инфраструктурой предприятия, особенностями бизнес-процессов, реальной ситуацией, при этом могут проводить оценку субъективно. Сторонние специалисты, наоборот, при независимой оценке могут недостаточно учитывать специфику и особенности деятельности организации. Экспертный подход основан на сборе, анализе и ранжировании оценок экспертов. На рисунке 1 представлена классификация методов экспертного подхода.

1. Методы группового опроса экспертов. Метод Паттерн предполагает коллективную работу экспертов, обсуждение мнений, совещаний, проводимых в несколько раундов, на каждом этапе опросов экспертов не меняют. Для метода Делфи главной особенностью является независимость экспертов и отсутствие влияния на их оценку, при этом каждый раз привлекают новых экспертов. Результаты такой работы подвергаются обработке методами статистического анализа, и формируется конечная оценка.

2. Математико-статистические методы обработки экспертных оценок основаны на проведении корреляционной оценки, расчете дисперсии, различного рода распределений и подразделяются на: ранжирование, метод парных сравнений, метод последовательных предпочтений, метод непосредственной оценки и другие.

3. Методы экспертной оценки показателей качества основаны на определении весомости того

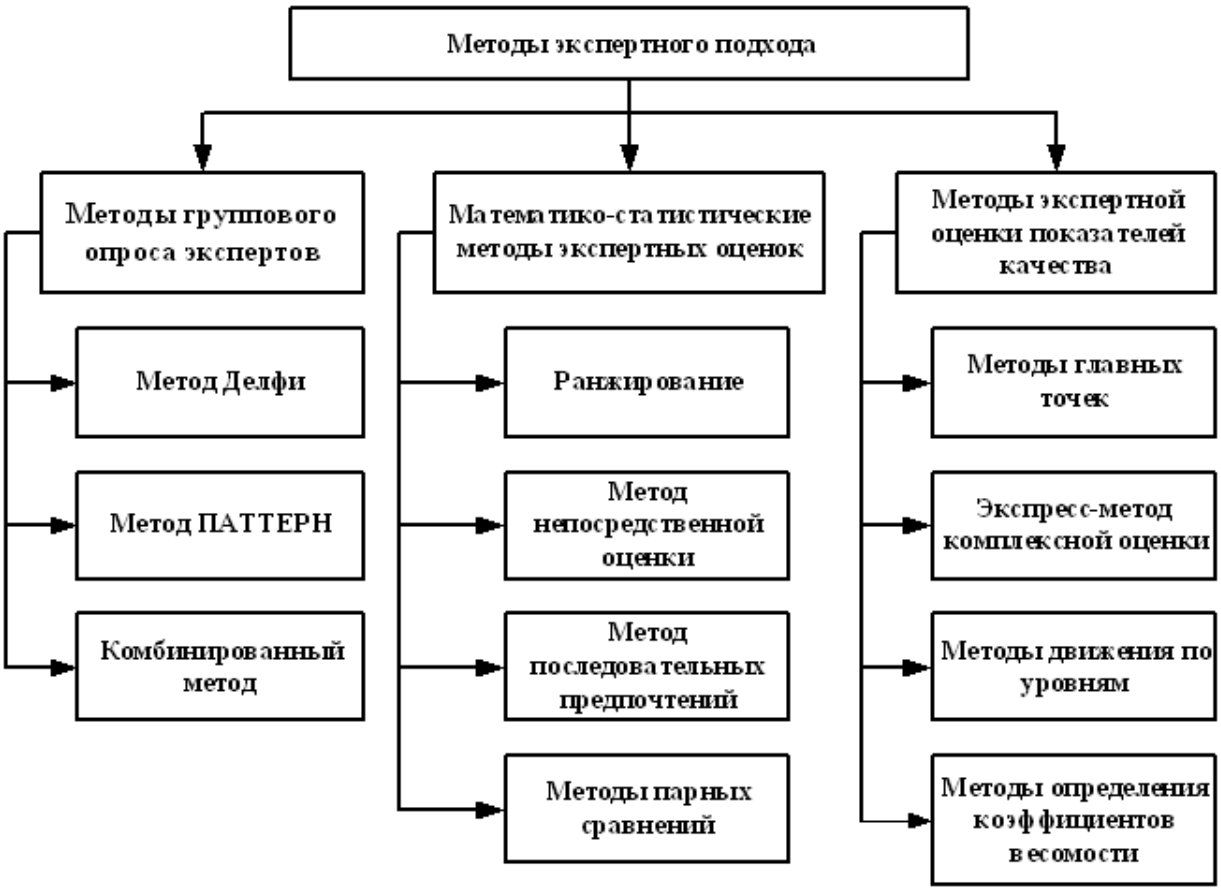


Рисунок 1. Классификация методов экспертного подхода

или иного критерия качества продукции или услуги. Применение данных методов целесообразно, если показателями качества выбраны конкретные физические величины и в наличии присутствуют измерительные приборы с заданными метрологическими параметрами.

Для нашего исследования был выбран класс математико-статистических методов обработки экспертных оценок, конкретно метод анализа иерархий (МАИ).

На первом этапе решения задачи с применением МАИ следует задать критерии оценки угроз. На втором этапе эксперты должны определить степень значимости критериев попарным сравнениям по 9-балльной шкале. Преимущество этого метода заключается в предоставлении возможности учета различных факторов, несопоставимых друг с другом, для этого проводится сравнение каждого критерия с каждым [3; 5].

Нами была разработана иерархическая модель определения актуальных угроз с использованием МАИ (рисунок 2).

На первом уровне представлены этапы процесса оценки угроз безопасности в соответствии с Методикой оценки угроз безопасности информации ФСТЭК России от 5 февраля 2021 года: негативные последствия, которые могут привести к ущербу для предприятия, перечень угроз, перечень объектов воздействия этих угроз, среди которых автоматизированные рабочие места, серверное оборудование, сетевые, интерфейсные компоненты и другие.

На втором уровне необходимо выделить критерии, уровень значимости которых должны оценить эксперты.

Третий уровень включает непосредственные значения оценки критериев в процентном отношении.

Согласно Методике ФСТЭК для определения угроз, актуальных для данной организации, необходимо определить источник угроз по возможному нарушителю, провести инвентаризацию всех активов для понимания объектов воздействия, рассмотреть все возможные уязвимости, реальные атаки на компьютерные системы, доступные из различных открытых источников, оценить возможные риски (ущерб) для владельцев информационных активов [1; 4]. Угрозу безопасности информации (УБИ) составляют следующие компоненты:

УБИi = [нарушитель (источник угрозы), объект воздействия, способы реализации угрозы; негативные последствия].

Модель угроз разрабатывается, как правило, группой экспертов, мнения которых могут не совпадать. При коллективном оценивании достоверность принятых решений следует обеспечить согласованностью с исключением необъективных завышенных или заниженных прогнозов.

Для решения возможных проблем оценки согласованности мнений экспертов применение только метода анализа иерархий является недостаточным. Необходимо определить согласованность оценок экспертов для достижения наибольшей достоверности принятого решения. Субъективные психологические факторы могут исказить полученные в ходе оценки результаты. Чтобы оценить уровень согласованности экспертных оценок предлагается вычислить для ран-

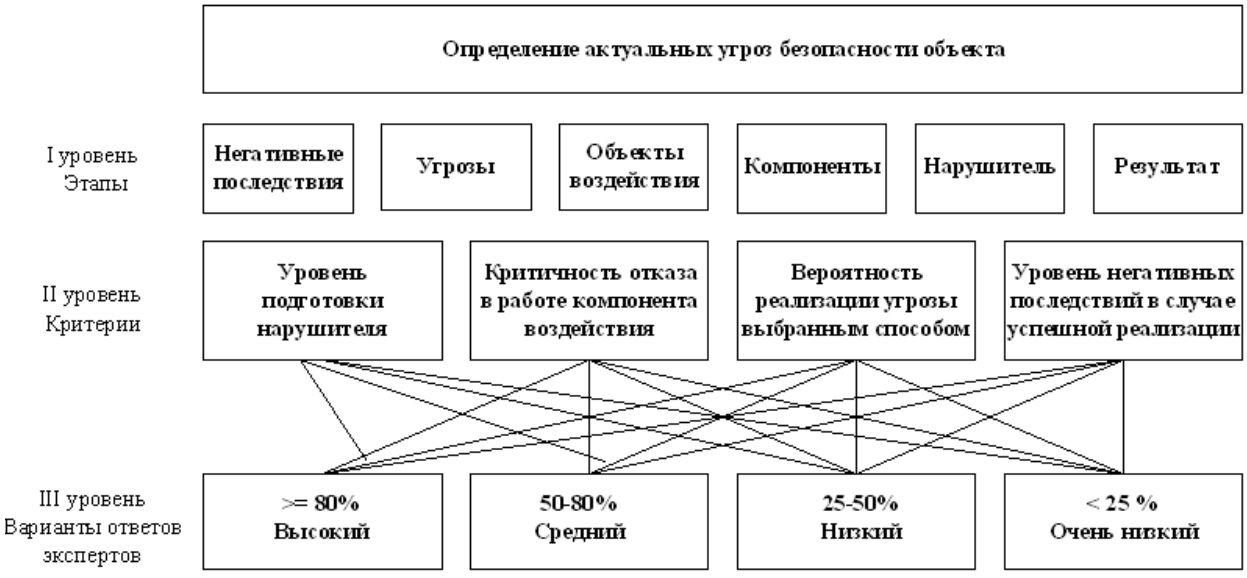


Рисунок 2. Иерархическая модель определения актуальных угроз

жированных данных коэффициент конкордации. При переходе этого коэффициента за заданный предел формируется результат о неслучайной согласованности оценок группы экспертов.

На рисунке 3 представлены алгоритмы определения согласованности экспертных мнений, включающие обработку полученных экспертных оценок в виде матрицы рангов, расчет коэффициента конкордации и расчет статистической значимости.

Приведенный выше алгоритм включает несколько ключевых этапов:

1. Формирование экспертной группы.
2. Определение показателей оценки и получение в соответствии с ними экспертного мнения.
3. Расчет математических показателей степени согласованности экспертного мнения.
4. Формирование результатов.

Первым этапом предлагаемого алгоритма является вопрос формирования экспертной группы. Этап требует четкой постановки задач в зависимости от рассматриваемого объекта защиты. Эксперты должны обладать достаточными компетенциями в различных аспектах информационной безопасности с учетом применяемых на объекте технических решений. Критерии отбора должны учитывать профессиональные квалификации и опыт.

Определение показателей оценки служит ключевым этапом в формировании мнения об актуальности угроз информационной безопасности [10]. На данном этапе должны быть выделены наиболее значимые характеристики субъекта оценки, совокупность которых будет являться основой для выработки стратегий защиты. Для предложенного алгоритма мнение экспертов выражается в количественной оценке, что позволяет провести обработку полученной информации с помощью математического метода.

На третьем этапе объективную оценку результата обеспечивает расчет коэффициента конкордации. Выбор граничного значения коэффициента напрямую влияет на результаты проведения опроса – значение коэффициента прямо пропорционально степени согласованности экспертного мнения. При расчете статистических показателей

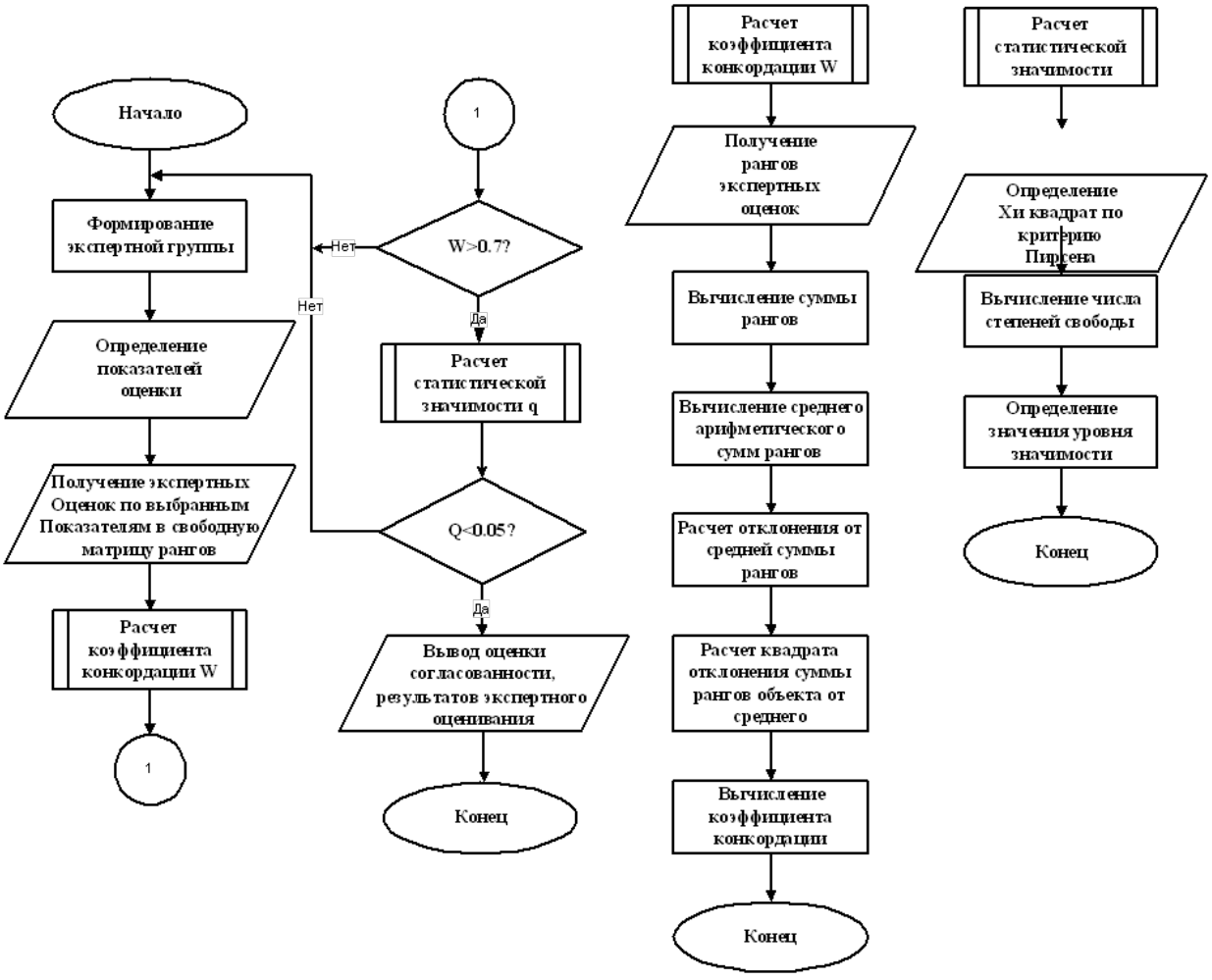


Рисунок 3. Алгоритмы определения согласованности экспертных мнений

также важно выполнение проверки результатов на вероятность случайного возникновения. Гипотеза о случайности полученных результатов проверяется в соответствии со значением критерия Пирсона, пороговое значение которого зависит от количества экспертов в опрашиваемой группе [6].

Результатами проведения опроса экспертной группы является обобщенный перечень актуальных угроз для рассматриваемого объекта защиты, а также результат оценки согласованности экспертных мнений. Предлагаемый алгоритм позволяет не только выполнить оценку угроз по выбранным характеристикам, но и сформировать единое экспертное мнение с допустимой степенью согласованности, основанное на компетенциях специалистов разных направлений в области информационной безопасности.

В соответствии с разработанными алгоритмами было проведено моделирование определения степени согласованности экспертных оценок, реализация осуществляется в программном средстве.

В качестве примера рассматривается группа из 4 экспертов. Для вывода результатов оценки сформирована шкала ранжирования из 4 значений: очень низкий, низкий, средний и высокий уровни. Далее выполняется опрос экспертов по каждому из четырех критериев: уровень подготовки нарушителя, критичность отказа в работе компонентов, вероятность реализации угрозы, уровень негативных последствий. Для разработки программного средства был проведен анализ аналогичных разработок, определены особенности, выявлены достоинства и недостатки, определены требования к разработке авторского программного средства. Новый раздел банка угроз ФСТЭК позволяет в интерактивном режиме осуществить формирование угроз безопасности по актуальной Методике [4]. На пересечении множеств угроз безопасности, объектов (компонентов) воздействий и способов реализации (нарушители) формируется УБИ. При этом отсутствует возможность провести коллективную оценку и проверить согласованность и достоверность мнений экспертов. Для автоматизации данных решений создана функциональная модель процесса определения актуальных угроз на основе экспертного подхода, которая позволяет учесть поступающие на вход данные об объекте защиты  получить результат наряду с перечнем актуальных УБИ, формировать отчет о согласованности экспертного мнения и дальнейшие рекомендации по корректировке действий экспертов [8]. Общая функциональная модель IDEF0 представлена на рисунке 4.

Декомпозиция процесса определения актуальных угроз включает пять последовательных этапов, первые четыре из которых проходит каждый эксперт отдельно, что позволяет осуществить дистанционный сбор мнений и результаты опроса загрузить в разрабатываемую программную систему.

На первом шаге производится выбор перечня объектов воздействия угроз, на основе которого определяется вероятный нарушитель и перечень характерных для него угроз. Затем определяются способы реализации выявленных на предыдущем этапе угроз. После этого выявляются сценарии воздействия угроз на объекты информатизации для сопоставления угроз и объектов воздействий. Для полученного списка угроз каждый эксперт определяет негативные последствий по уровню ущерба для каждой угрозы. Составленные каждым экспертом по отдельности перечни векторов

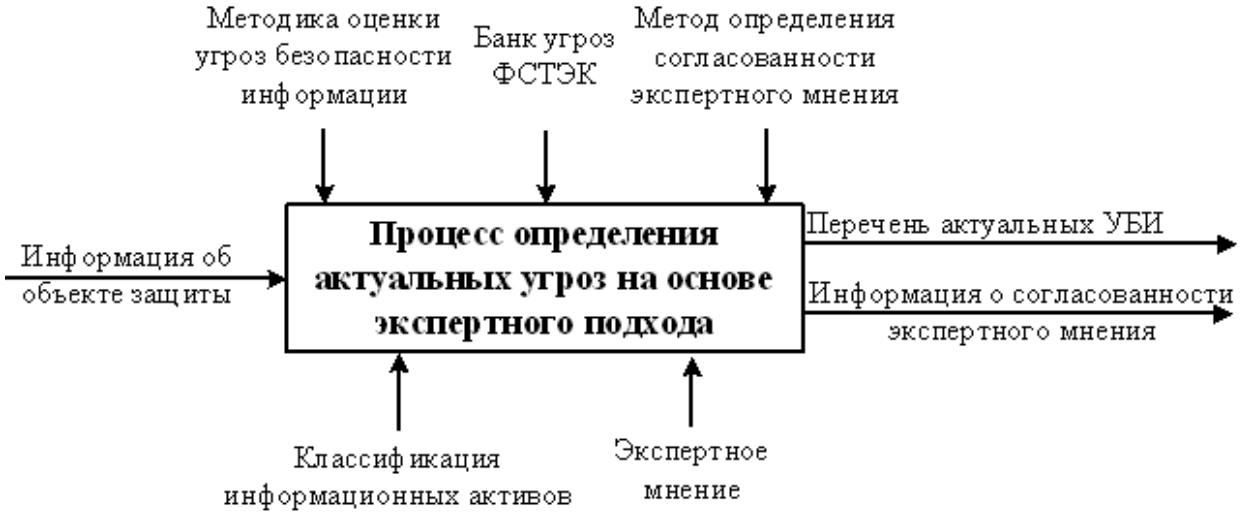


Рисунок 4. Общая функциональная модель разрабатываемого метода

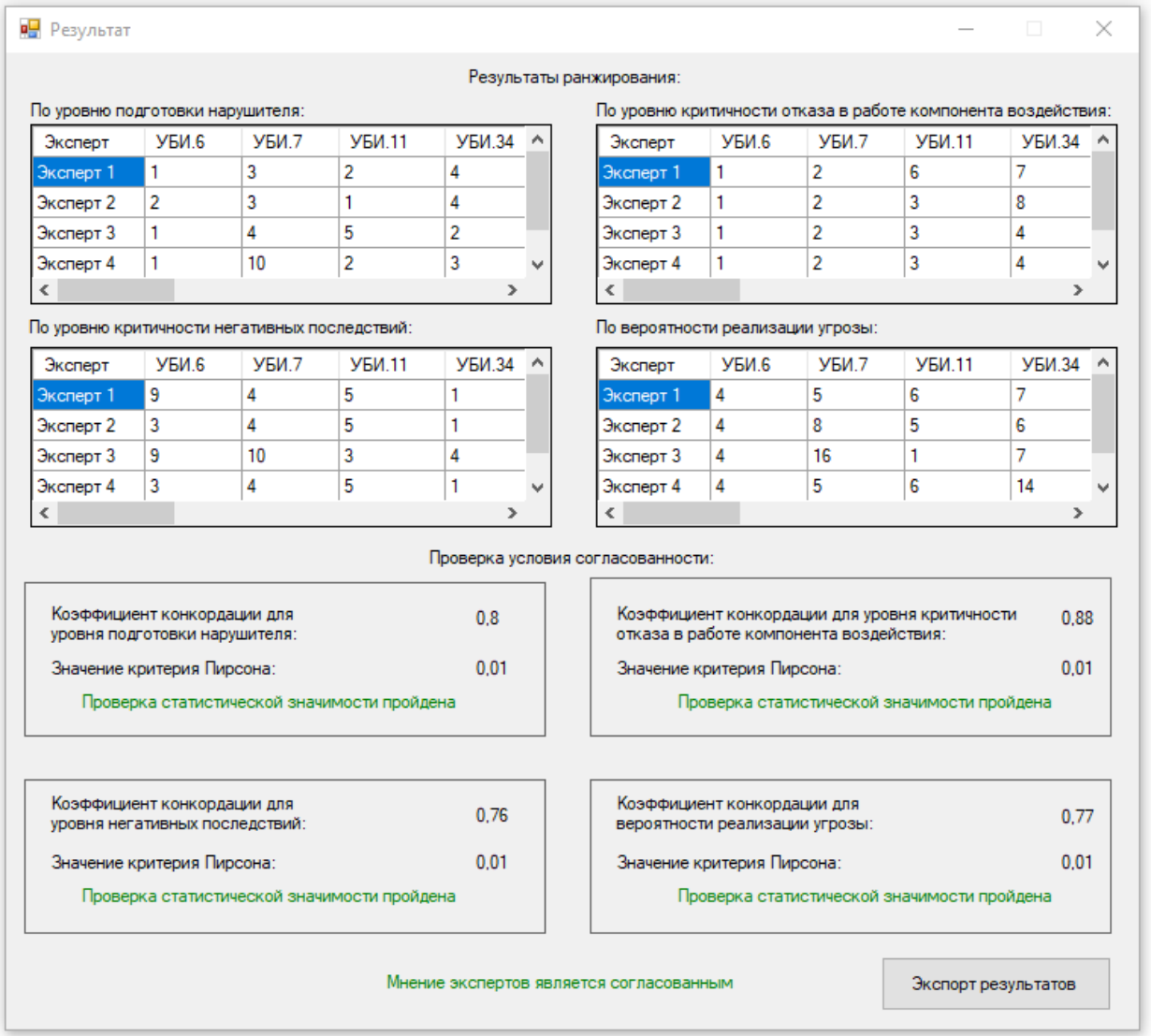


Рисунок 5. Экранная форма вывода результата опроса экспертной группы

угроз являются входными данными для определения согласованности экспертного мнения.

Расчет коэффициента конкордации является заключительным этапом и позволяет определить согласованность мнений экспертов и уровень значимости для принятия объективного решения.

На экранной форме разработанного программного средства представлены результаты расчета коэффициента конкордации, значения которого превышают критическое значение (0,7) и результаты расчета уровня значимости (рисунок 5).

## Вывод

Были разработаны иерархическая модель определения актуальных угроз с использованием экспертного подхода, а также алгоритмы определения степени согласованности экспертных оценок в задаче определения актуальных угроз объекта информатизации, что позволило повысить эффективность построения рациональной системы безопасности информации именно от актуальных угроз, так как от всех угроз построить защиту невозможно, да и нецелесообразно. Предложенный подход позволяет уменьшить процент потенциально неучтенных угроз за счет использования классификации информационных активов и проверки согласованности экспертного мнения. На основе представленных моделей и алгоритмов разработано программное средство для автоматизированной оценки угроз информационной безопасности и определения согласованности полученных результатов.

## Литература

1. Банк данных угроз безопасности информации. Федеральная служба по техническому и экспортному контролю. URL: https://bdu.fstec.ru/threat (дата обращения: 17.01.2024).

2. Дивина Т.В., Петракова Е.А., Вишневский М.С. Основные методы анализа экспертных оценок. Экономика и бизнес: теория и практика. 2019. №7. С. 42–44.
3. Бурькова Е.В., Рычкова А.А. Методика принятия решений при выборе средств физической защиты на основе метода анализа иерархий // Научно-технический вестник Поволжья. 2021. № 5. С. 119–123.
4. Методика оценки угроз безопасности информации: методический документ. Москва: ФСТЭК. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 17.01.2024).
5. Рычкова А.А., Клиндух В.О. Оценка эффективности защитных мер персональных данных в учебном заведении на основе метода анализа иерархий // Новые импульсы развития: вопросы научных исследований. 2021. С. 58–66.
6. Письменская А.А., Гостюнин Ю.А., Давидюк Н.В. Согласованность мнений экспертов при оценке рисков информационной безопасности с применением АВС-анализа // Математические методы в технике и технологиях (ММТТ). 2020. № 7. С. 55–57.
7. Смирнов Р.А., Новиков С.Н. Анализ методик оценки угроз безопасности информации // Телекоммуникации. 2023. № 7. С. 24–27.
8. Степанов В.А., Андреев Н.Д. Моделирование угроз безопасности информации по новой методике ФСТЭК, используя средства автоматизации // Информационные технологии. Проблемы и решения. 2021. № 4 (17). С. 95–101.
9. Филиппов Н.В., Киреева Н.В., Поздняк И.С. Подход к созданию экспертной системы оценки информационной безопасности телекоммуникационных систем // Электросвязь. 2022. № 2. С. 61–66.
10. Kotenko I., Parashchuk I. Analysis of threats to information security of industrial automation systems using euclidean and hamming distances between fuzzy sets // Conference Proceedings: International Russian Automation Conference (RusAutoCon). 2023. P. 13–18.

*Получено 18.01.2024*

**Рычкова Анастасия Александровна,** к.п.н., доцент кафедры вычислительной техники и защиты информации (ВТиЗИ) Оренбургского государственного университета (ОГУ). 460018, Российская Федерация, г. Оренбург, Проспект Победы, 13. Тел. +7 922 535-32-45. E-mail: rnansy@yandex.ru

**Долгушев Никита Александрович,** студент кафедры ВТиЗИ ОГУ. 460018, Российская Федерация, г. Оренбург, Проспект Победы, 13; системный инженер Оренбургского филиала ООО «Уральский центр систем безопасности». 460021, Российская Федерация, г. Оренбург, ул. Луговая, 55. Тел. +7 951 032-77-91. E-mail: dolgushevn1@yandex.ru

**Бурькова Елена Владимировна,** к.п.н., доцент, доцент кафедры ВТиЗИ ОГУ. 460018, Российская Федерация, г. Оренбург, Проспект Победы, 13. Тел.+7 903 360-77-92. E-mail: tulpan63@bk.ru

**Коннов Андрей Леонидович,** к.т.н., доцент, доцент кафедры ВТиЗИ ОГУ. 460018, Российская Федерация, г. Оренбург, Проспект Победы, 13; доцент кафедры математических и естественно-научных дисциплин Оренбургского филиала Поволжского государственного университета телекоммуникаций и информатики. 460022, Российская Федерация, г. Оренбург, ул. Пролетарская/Юркина, 249/76. Тел. +7 912 844-91-91. E-mail: andrey_konnov@mail.ru

## MODELS AND ALGORITHMS FOR IDENTIFYING CURRENT THREATS BASED ON AN EXPERT APPROACH

*RichkovaA.A.[1], DolgushevaN.A.[1,3], Burkova E.V.[1], Konnov A.L.[1,2]*

*[1]Orenburg State University, Orenburg, Russian Federation*

*[2]Orenburg Branch of the Povolzhskiy State University of Telecommunications and Informatics, Orenburg, Russian Federation*

*[3]Orenburg Branch of the Ural Center of Security Systems, Orenburg, Russian Federation*

*E-mail: rnansy@yandex.ru, dolgushevn1@yandex.ru, tulpan63@bk.ru, andrey_konnov@mail.ru*

The task of identifying current security threats is becoming increasingly important, due to the increase in the volume of processed information of limited access, an increase in the number of all kinds of threats, and an increase in the potential of violators. At enterprises and organizations in various sectors of the

economy, specialists regularly conduct information security audits in order to identify vulnerabilities and ultimately to prevent possible negative consequences. To build a rational information security system at the facility, it is important to organize protection against actual threats, since it is impossible to build protection against all threats, and it is impractical. The article proposes models and algorithms for determining current threats based on an expert approach, which can become the basis for the development of an automated system for making reliable decisions in the tasks of protecting informatization objects.

***Keywords:*** *security threat, hierarchy analysis method, hierarchical model*

**DOI:** 10.18469/ikt.2023.21.3.05

**Rychkova Anastasia Aleksandrovna,** Orenburg State University, 13, Pobedy Avenue, Orenburg, 460018, Russian Federation; Associate Professor of Computer Science and Information Security Department, PhD in Pedagogical Sciences. Tel. +7 922 535-32-45. E-mail: rnansy@yandex.ru

**Dolgushev Nikita Aleksandrovich,** Orenburg State University, 13, Pobedy Avenue, Orenburg, 460018, Russian Federation; Student of Computer Science and Information Security Department. Orenburg Branch of the Ural Center of Security Systems, 55, Lugovaya Street, Orenburg, 460021, Russian Federation; System engineer. Tel. +7 951 032-77-91. E-mail: dolgushevn1@yandex.ru

**Burkova Elena Vladimirovna,** Orenburg State University, 13, Pobedy Avenue, Orenburg, 460018, Russian Federation; Associate Professor of Computer Science and Information Security Department, PhD in Pedagogical Sciences. Tel. +7 903 360-77-92. E-mail: tulpan63@bk.ru

**Konnov Andrey Leonidovich,** Orenburg State University, 13, Pobedy Avenue, Orenburg, 460018, Russian Federation; Associate Professor of Computer Science and Information Security Department, PhD in Technical Sciences. Orenburg Branch of the Povolzhskiy State University of Telecommunications and Informatics, 249/76, Proletarskaya/Urkina Street, Orenburg, 460022, Russian Federation; Associate Professor of Mathematical and Natural Science Disciplines Department. Tel. +7 912 844-91-91. E-mail: andrey_konnov@mail.ru

**References**

1. Database of information security threats. federal service for technical and export control. URL: https://bdu.fstec.ru/threat (accessed: 17.01.2024). (In Russ.)
2. Divina T.V., Petrakova E.A., Vishnevsky M.S. Basic methods of analysis of expert assessments. *Ekonomika i biznes: teoriya i praktika*, 2019, no. 7, pp. 42–44. (In Russ.)
3. Burkova E.V., Rychkova A.A. Method of decision-making system for the selection of physical protection means based on the hierarchy analysis method. *Nauchno-tekhnicheskij Vestnik Povolzh'ya*, 2021, no. 5, pp. 119–123. (In Russ.)
4. *Methodology for Assessing Information Security Threats: Methodological Document*. Moscow: FSTEC. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (accessed: 17.01.2024). (In Russ.)
5. Rychkova A.A., Klindukh V.O. Evaluation of the effectiveness of protective measures of personal data in an educational institution based on the method of hierarchy analysis. *Novye impul'sy razvitiya: voprosy nauchnyh issledovanij*, 2021, pp. 58–66. (In Russ.)
6. Pishevskaya A.A., Gostyunin Yu.A., Davidyuk N.V. Agreement of opinions of experts in the assessment of risks of information security with application of abc analysis. *Matematicheskie metody v tekhnike i tekhnologiyah (MMTT)*, 2020, no. 7, pp. 55–57. (In Russ.)
7. Smirnov R.A., Novikov S.N. Analysis of assessment methods of information security threats. *Telekommunikacii*, 2023, no. 7, pp. 24–27. (In Russ.)
8. Stepanov V.A., Andreev N.D. Modeling information security threats using the new FSTEC methodology using automation tools. *Informacionnye tekhnologii. Problemy i Resheniya*, 2021, no. 4 (17), pp. 95–101. (In Russ.)
9. Filippov N.V., Kireeva N.V., Pozdnyak I.S. Approach to creating an expert system for

assessing the information security of telecommunication systems. *Elektrosvyaz'*, 2022, no. 2, pp. 61–66. (In Russ.)
10. Kotenko I., Parashchuk I. Analysis of threats to information security of industrial automation systems using euclidean and hamming distances between fuzzy sets. *Conference Proceedings: International Russian Automation Conference (RusAutoCon)*, 2023, pp. 13–18. (In Russ.)

*Received 18.01.2024*

УДК 004.7; 372.862

# СПЕЦИАЛИСТ ПО ЭКСПЛУАТАЦИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ: ЗНАНИЯ, УМЕНИЯ, НАВЫКИ

*Галич С.В., Сафонова О.Е.*
*Волгоградский государственный университет, Волгоград, РФ*
*E-mail: galich.sv@volsu.ru*

В статье проведен анализ российских разработок в сфере программно-конфигурируемых сетей, профессио-нального стандарта и вакансий с целью определения требуемых от специалистов знаний, умений, навыков. Показано, что рынок труда испытывает явную потребность в кадрах, способных эксплуатировать и разрабатывать решения, функционирующие на основе принципов программно-конфигурируемых сетей. Сделаны выводы о том, что наблюдается недостаток пособий практической направленности для подготовки специалистов в данной сфере, а также предложены возможные темы лабораторных работ для учебных пособий. Данная статья может быть полезна преподавателям образовательных учреждений средне-специального и высшего образования, а также дополнительного профессионального образования при разработке рабочих программ дисциплин, лекций и лабораторных практикумов, посвященных программно-конфигурируемым сетям, а также обучающимся вышеупомянутых образовательных учреждений при планировании индивидуального плана обучения, выпускникам и молодым специалистам при планировании своего профессионального и карьерного развития.

***Ключевые слова:*** *программно-конфигурируемые сети, виртуализация сетевых функций, знания, умения, навыки, образование*

## Введение

В 2022 году уход с российского рынка крупнейших мировых производителей сетевого оборудования, аннулирование ими в одностороннем порядке действующих лицензий и прекращение технической поддержки закупленного оборудования продемонстрировали уязвимость набравшей популярность сервисной модели предоставления услуг и оборудования.

Сетевые устройства со встроенными интеллектуальными функциями, такие как межсетевые экраны нового поколения (NGFW), по воле производителя лишались большей части своего функционала быстрее, чем администраторы успевали предпринять какие-либо действия. Особо уязвимы оказались устройства, функционирующие в соответствии с принципами технологии программно-конфигурируемых сетей (ПКС, англ. SDN), подразумевающей отделение плоскости управления (англ. control plane) от плоскости передачи (англ. data plane), при этом плоскость управления в лице SDN-контроллера совершенно не обязательно территориально располагать в центре обработки данных (ЦОД) или серверной эксплуатирующей организации. SDN-контроллер вполне может функционировать в облаке производителя устройства, более того, подобный подход в ряде случаев может быть выгодным для потребителя с точки зрения затрат и лицензирования, а именно позволяет реализовать одно из достоинств SDN как концепции и переводить капитальные затраты на оборудование в операционные [1].

В крайне деструктивных действиях была замечена компания Cisco: например, компания не ограничилась отключением устройств Cisco Meraki от облачных сервисов, но и захватила контроль над устройствами на территории Российской Федерации и создала открытый SSID (Service Set Identifier) вида «12345-Sanctions». Продукты серии Cisco vEdge SD-WAN (Software-Defined Networking in a Wide Area Network, программно-определяемая глобальная сеть)имеют целый набор различных проблем: от невозможности добавить новое устройство до истекших 9 мая 2023 года сертификатов безопасности, приводящих к неработоспособности устройств после перезагрузки и обновление которых невозможно без обращения в поддержку производителя (который, опять же, ушел с российского рынка).