УДК 681.513(045)
DOI 10.22213/2410-9304-2018-4-169-175

ОСОБЕННОСТИ РЕАЛИЗАЦИИ СИСТЕМЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ КРИТИЧЕСКИ ВАЖНЫХ И ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ НА ОСНОВЕ МЕТОДА КЛЕМЕНТСА – ХОФФМАНА

И. М. Янников, доктор технических наук, доцент, ИжГТУ имени М.Т. Калашникова, Ижевск, Россия
М. В. Телегина, кандидат технических наук, доцент, ИжГТУ имени М. Т. Калашникова, Ижевск, Россия

В статье дана оценка существующих подходов к проблеме оценки защищенности опасных объектов. Поскольку существующие методики не обеспечивают возможность применения единого системного подхода к оценке защищенности КВО, ПОО и территорий, предлагается проводить оценку с использованием системы моделирования и расчета состояния защищенности опасных объектов разработанной на основе метода Клементса – Хоффмана, в котором для описания системы защиты с полным перекрытием используется множество угроз, механизмов защиты и объектов защиты. Данная система при вводе данных о каких-либо угрозах и соответствующих средствах защиты может применяться для расчета любого вида защищенности опасных объектов.

В форме вывода результатов отображается пятизвенный (при необходимости и трехзвенный) граф со сформированными пользователем связями, расчетные матрицы, результаты их свертки и результаты расчета защищенности объекта.

Для расчета физической защищенности КВО и ПОО использовалась СУБД PostgreSQL, обладающая большим потенциалом для хранения и управления данными. Система реализована на C#.NET с применением пакета Microsoft .NET Framework 4.5.2.

В статье приводятся модель защитной системы с полным перекрытием, функциональные модели, служащие для формализованного описания процессов, типовая модель системы физической защиты КВО и ПОО, основные параметры и этапы разработки и тестирования осуществленного путем сравнения результатов работы системы с данными, полученными путем ручного расчета.

Ключевые слова: критически важный объект, потенциально опасный объект, метод Клементса – Хоффмана, система защиты.

Введение

В связи с ростом природных и антропогенных опасностей для функционирования социальных и производственных объектов в настоящее время представляется крайне актуальным вопрос повышения уровня всесторонней защищенности критически важных и потенциально опасных объектов (КВО и ПОО) от внутренних и внешних угроз. Повышение уровня защищенности невозможно без ее постоянной и объективной оценки. В то же время с развитием науки и высоких технологий становится все труднее спроектировать экономически выгодную систему защищенности опасных объектов, способную эффективно противостоять возникающим угрозам [1, 2].

Анализ существующих методик оценки и анализа рисков

В настоящее время создано множество систем управления рисками, каждая из которых оценивает риск по различным параметрам (вероятность угрозы, возможный ущерб, тяжесть последствий и др.). Используемые при этом методики относительно неэффективны, поскольку единый централизованный контроль в этой сфере практически отсутствует [3]. Это исключает возможность применения единого системного подхода в оценке безопасности не только объектов, но и территории.

Известные методики оценки и анализа рисков можно разделить [4, 5]:

– на методики, использующие качественные оценки;

– методики, использующие количественные оценки;

– методики, использующие смешанные оценки.

В первом случае, например по экспертным шкалам, возможно с минимальной затратой ресурсов провести анализ причин возникновения рисков, последствия их реализации, однако в любом случае шкала будет носить субъективный характер и возникнут проблемы сравнения угроз одной категории.

При количественной оценке сравнительный анализ будет более точен, однако не учитываются причины и последствия возникновения рисков, данная оценка не всегда возможна, и зачастую ранжирование рисков экспертами становится более эффективно.

Таким образом, использование смешанных оценок позволяет провести наиболее всесторон-

нее решение задачи создания оценки управления рисками.

В существующих в настоящее время методиках оценки системы защиты для проектирования системы защиты применяется математическое моделирование, с разделением процесса создания систем защиты на отдельные этапы: ранжирование угроз; анализ механизмов защиты и пр. При этом единого метода оценки защищенности не существует, что связано с трудностью формализации данной проблемы.

Большую часть применяемых методик объединяет узконаправленность данных системы и необходимость специальной подготовки. Заказчик, как правило, не знаком с такими программами, и ему приходится пользоваться услугами оператора разработчика. Естественно, что качество выдаваемых оценок полностью зависит от уровня эксперта, способного при наличии соответствующей квалификации решить задачу вручную. Именно поэтому экспертные оценки, как выполненные вручную, так и с применением программных средств, зачастую имеют один и тот же уровень точности.

Описание предлагаемой системы оценки на основе модели Клементса – Хоффмана

Таким образом, исходя из цели – автоматизации процессов выбора технических средств и способов повышения защищенности опасных объектов – предлагается система оценки защищенности КВО и ПОО с возможностью формирования перечней угроз, объектов защиты и средств защиты, а также расчетом защищенности указанных объектов на основе применения модели Клементса – Хоффмана.

В методе Клементса – Хоффмана, в отличие от других, при формировании модели с полным перекрытием угроз оценивается ущерб для каждой угрозы [6]. В связи с чем для оценки физической защищенности критически важных и потенциально опасных объектов использован метод Клементса – Хоффмана, до этого применявшийся только для решения задач информационной безопасности [7, 8].

Для описания системы защиты с полным перекрытием использованы следующие множества: угрозы; механизмы защиты; объекты защиты, уязвимые места, барьеры (рис. 1). Выбор вышеуказанной модели обусловлен возможностью оценки защищенности системы, выявления величины ущерба при осуществлении угрозы и определении оптимального варианта проектируемой системы защиты КВО и ПОО [9].

Расчет защищенности КВО и ПОО представляет собой процесс получения данных об индексе защищенности объекта и ожидаемом ущербе от осуществления угрозы. Данные действия система выполняет автоматически, эксперту в области безопасности необходимо проверить полученные данные и в случаи необходимости вернуться к этапу моделирования.

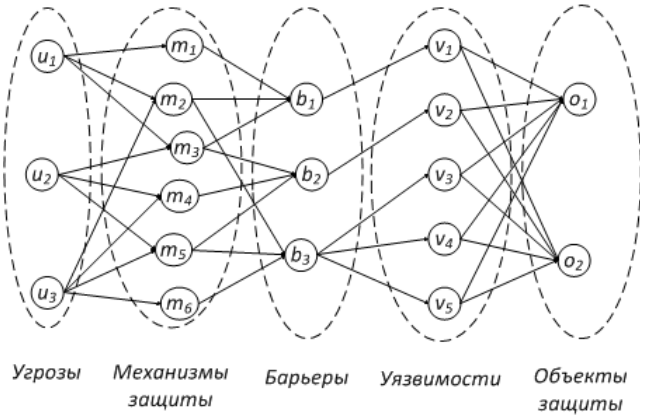

Рис. 1. Модель защитной системы с полным перекрытием

На рис. 2 приведена функциональная модель IDEF0, служащая для формализованного описания упомянутых выше процессов.

Модель системы описывает ключевые процессы, отношения между руководством объектов и экспертом в области безопасности, а также точки принятия решения в системе.

На рис. 3 приведена диаграмма расчетов, служащая для понимания логики процессов, присутствующих в системе, и являющаяся подготовительным этапом для разработки системы.

Разработка тестового набора данных служит для тестирования работы системы физической защищенности КВО и ПОО. Данный тестовый набор данных разбит на 5 ключевых групп: угрозы; механизмы защиты; барьеры; уязвимости; типовые объекты предприятия.

Данные наборы данных будут использоваться как контрольные наборы для системы, в дальнейшем администратор сможет задать свой набор данных.

Типовая модель системы физической защиты (СФЗ) представлена на рис. 4.

Для расчета физической защищенности КВО и ПОО использовалась СУБД PostgreSQL, обладающая большим потенциалом для хранения и управления данными. Работа администратора системы значительно упрощена за счет большого количества разработанных графических интерфейсов. Данная база данных позволяет получать расчетное значение ущерба от осуществления каждой угрозы, сохранять значения для использования в других проектах.

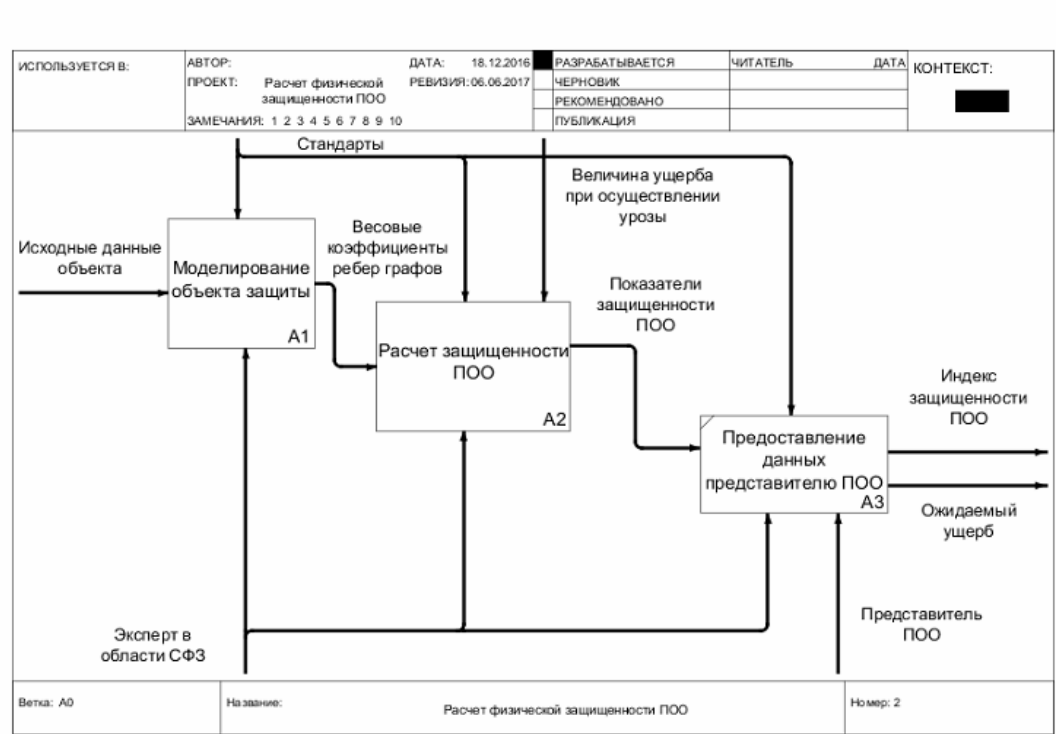

Рис. 2. Декомпозиция блока «Расчет защищенности ПОО»

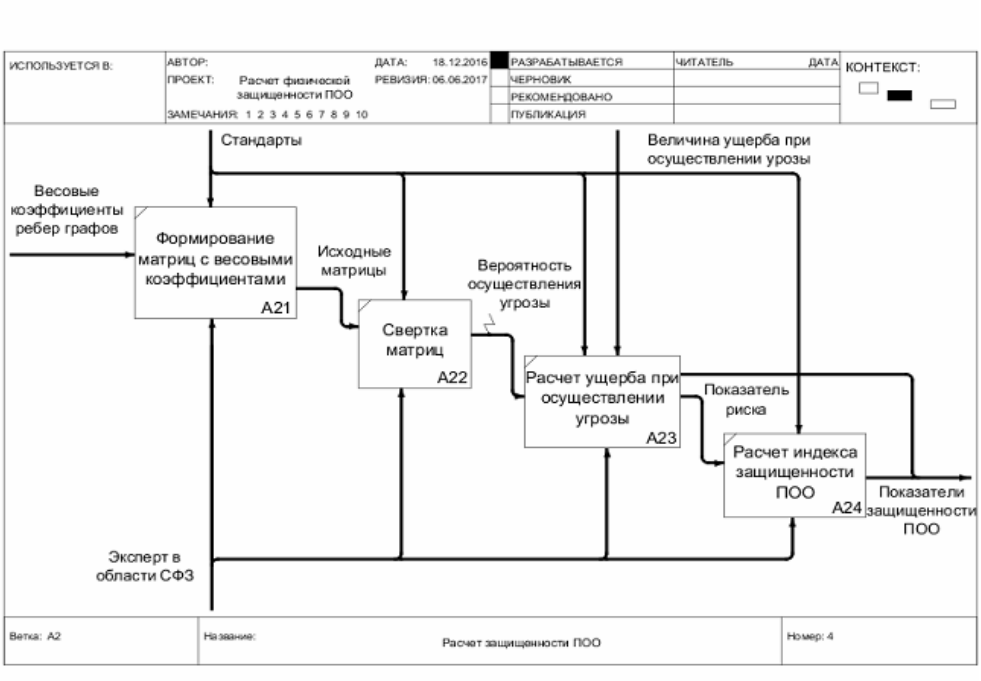

Рис. 3. Декомпозиция блока «Расчет физической защищенности»

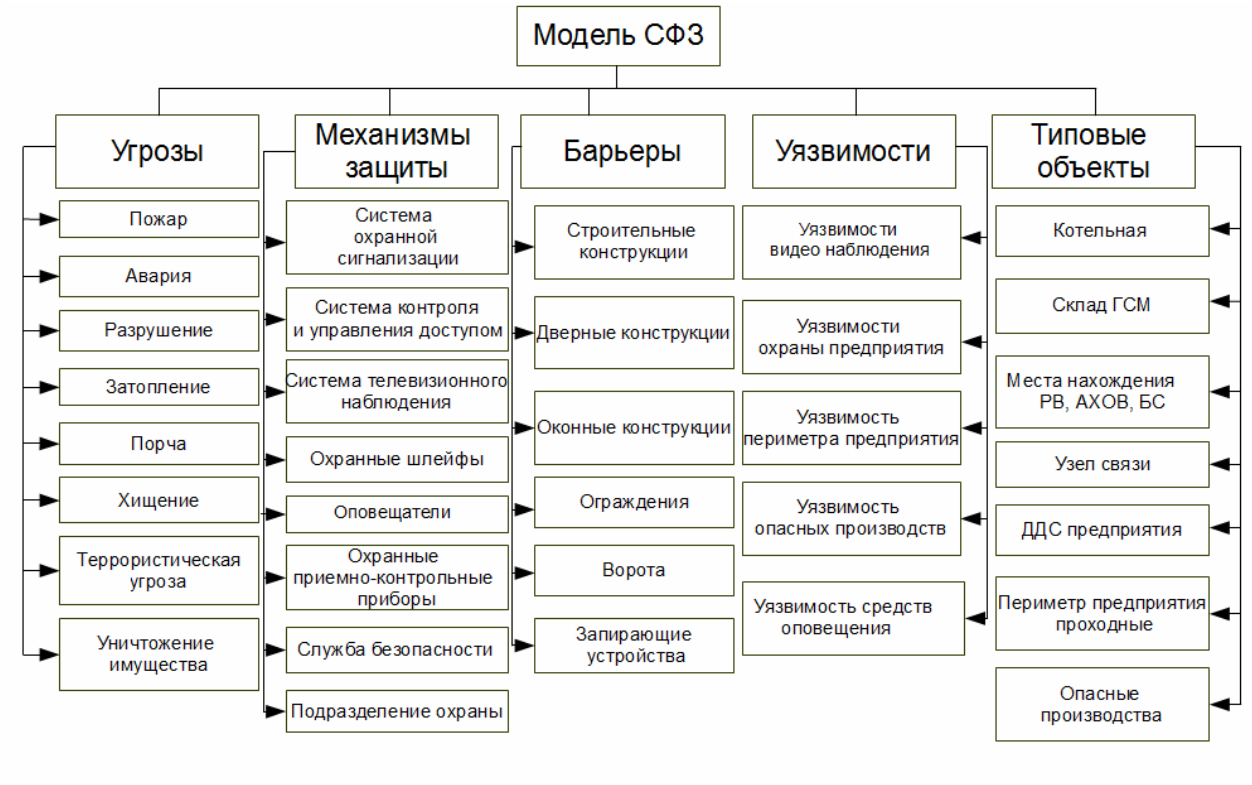

Рис. 4. Типовая модель СФЗ КВО и ПОО

Система реализована на C#.NET с применением пакета Microsoft .NET Framework 4.5.2, что обусловлено следующими качествами данной среды разработки: кроссплатформенностью, мощной библиотекой классов, возможностью написания модулей приложения на разных языках программирования, большим количеством справочной информации и готовых библиотек.

Принцип работы приложения заключается в том, что вначале специалист в области безопасности настраивает классификаторы угроз, механизмов защиты, барьеров, уязвимостей, объектов. Когда классификаторы настроены и для всех вариантов введены весовые коэффициенты, пользователь может приступить к созданию проекта. Он дает наименование проекту, указывает тип предприятия, для которого проводится анализ, выбирает экземпляры из классов угроз, механизмов защиты, барьеров, уязвимостей и объектов. В итоге система формирует заполненный граф, показывая промежуточные и итоговые матрицы, а также рассчитывает сумму ущерба по каждой из угроз и общий коэффициент защищенности объекта. На рис. 5–9 показана программная реализация проекта.

В форме создания проекта (рис. 5) вводится наименование проекта, выбирается тип проекта, при необходимости вводится описание.

На рис. 6 показано окно справочника «Угроз». Здесь производится добавление новых угроз, выбор класса опасности и значение величины ущерба. Для каждой угрозы задаются весовые коэффициенты механизмов защиты. На рис. 7 – окно справочника «Механизмы защиты», в котором производится добавление новых механизмов защиты, выбор их типов и добавление описания. Для каждого механизма защиты в нижней вкладке задаются весовые коэффициенты барьеров, объектов или угроз.

Аналогичным образом осуществляется работа со справочниками барьеров, уязвимостей, объектов.

В форме вывода результатов (рис. 8) отображается пятизвенный (при необходимости и трехзвенный) граф со сформированными пользователем связями, расчетные матрицы, результаты их свертки и результаты расчета защищенности объекта.

Заключение

Результаты тестирования разработанной системы показали ее способность успешно формировать графическую модель системы защиты КВО и ПОО, осуществлять необходимые расчеты защищенности. Справочники элементов системы защиты позволяют успешно формировать весовые коэффициенты, используемые при расчетах. Результаты расчетов были протестированы путем сравнения результатов работы системы с данными, полученными путем ручного расчета.

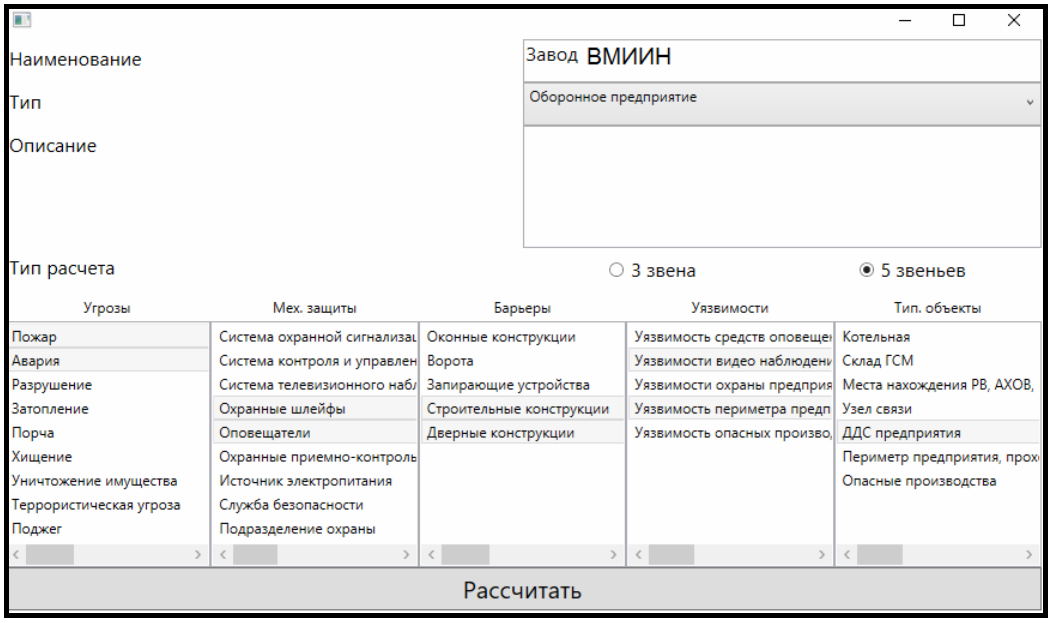

Рис. 5. Создание проекта

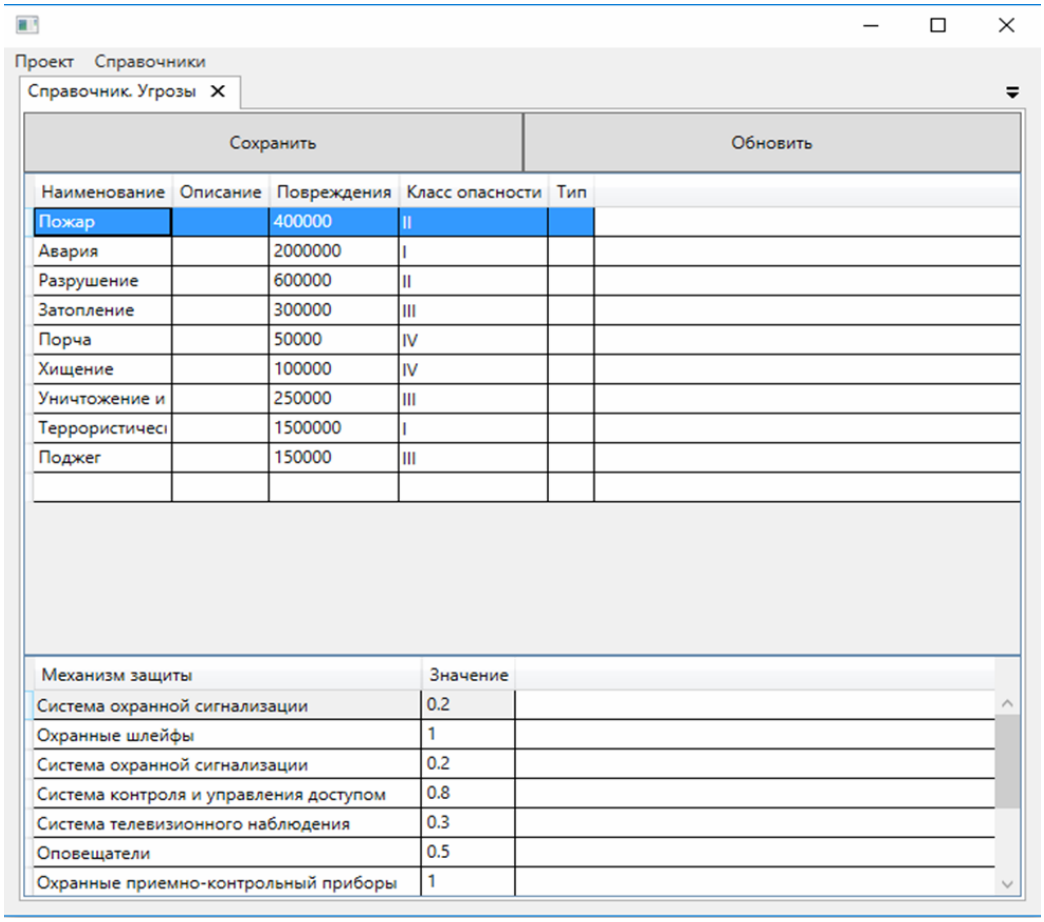

Рис. 6. Справочник «Угрозы»

Предлагаемая система при вводе данных о соответствующих угрозах, критериях, параметрах и средствах защиты может применяться для расчета любых видов защищенности критически важных и потенциально опасных объектов, что позволит на практике реализовать системный подход к обеспечению безопасности.

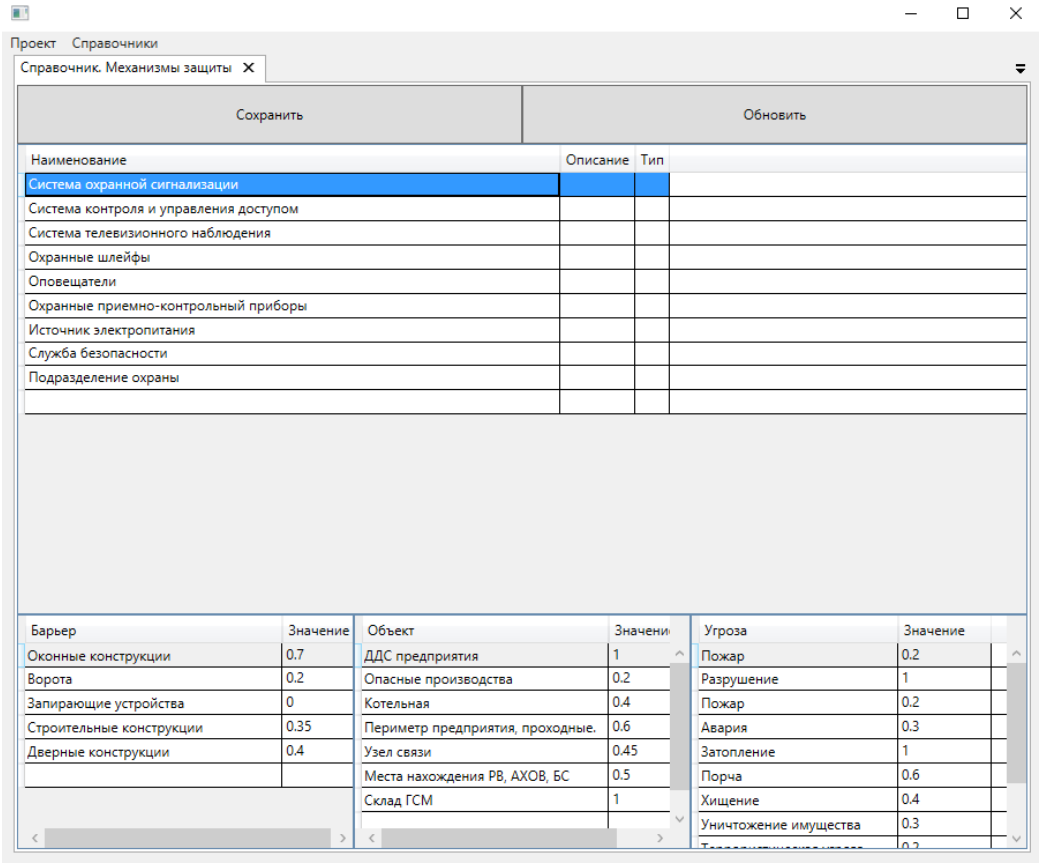

Рис. 7. Окно справочника «Механизмы защиты»

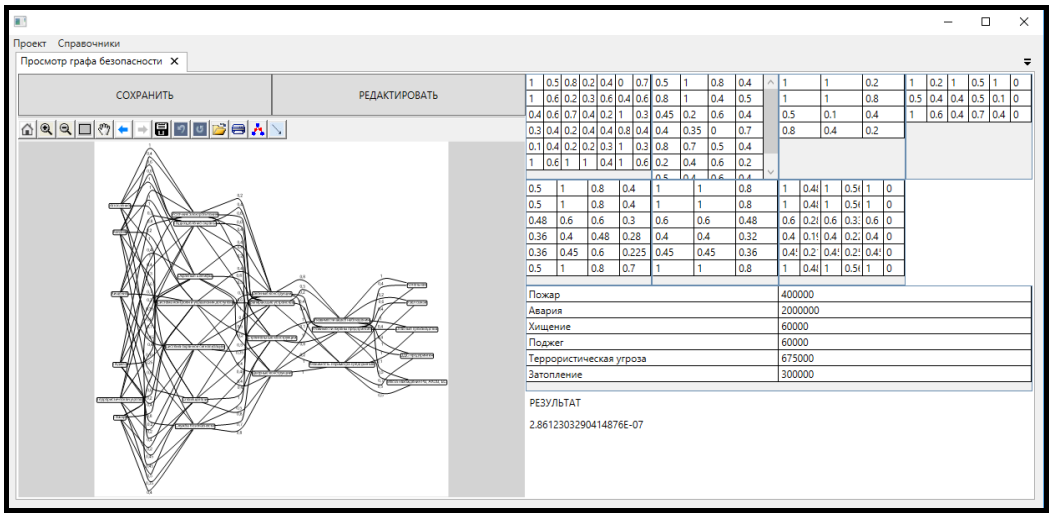

Рис. 8. Форма вывода результатов

Библиографические ссылки

1. *Янников И. М., Телегина М. В., Габричидзе Т. Г.* Комплексный подход к организации мониторинга защищенности потенциально опасных объектов с использованием ГИС-технологий // Интеллектуальные системы в производстве. 2015. № 3 (27). С. 83–87.

2. *Куделькин В. А., Янников И. М., Телегина М. В.* Принципы создания интегрированных систем безопасности критически важных и потенциально опасных объектов // Интеллектуальные системы в производстве. 2017. Т. 15, № 1. С. 105–109.

3. *Никитин Н. А., Ивахнюк Г. К., Трофимов И. В.* Основы обеспечения безопасности на потенциально опасных объектах обращения нефтепродуктов // Вестник Санкт-Петербургского университета ГПС МЧС России (электронный вариант СМИ). С. 27–31. URL: http://vestnik.igps.ru/wp-content/uploads/V53/6.pdf.

4. Национальный стандарт Российской Федерации ГОСТ ИСО/МЭК 31010:2009. Менеджмент риска. Методы оценки риска.

5. *Максименко В. Н., Ясюк В. Е.* Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. 2017. № 2. С. 42–48.

6. *Хоффман Л. Д.* Современные методы защиты информации / под ред. В. А. Герасименко. М. : Сов. радио, 1980. 264 с.

7. *Аверченков В. И., Рытов М. Ю., Гайнуллин Т. Р.* Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса – Хоффмана // Вестник Брянского ГТУ. 2008. № 1. С. 61–67.

8. *Рытов М. Ю., Луценко И. В.* Реализация системы проектирования защиты данных для малого предприятия // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : материалы X Межрегиональной научно-практической конференции [Электронный ресурс]. Брянск : БГТУ, 2018. С. 151–156. URL: Бесплатная электронная библиотека. http: konf.x-pdf.ru/19tehnicheskie/213514-1 (дата обращения: 15.08.2018).

9. Модели и методы оценки безопасности критически важных и потенциально опасных объектов / М. В. Телегина, И. М. Янников, В. А. Куделькин, И. С Ушаков // Интеллектуальные системы в производстве. 2017. Т. 15, № 1. С. 118–121.

References

1. Yannikov I.M., Telegin M.V., Gabrichidze T.G. [An integrated approach to the organization of monitoring the security of potentially hazardous objects using GIS technologies]. *Intellektual'nye sistemy v proizvodstve*. 2015. No. 3. Pp. 83-87 (in Russ.).

2. Kudelkin V.A., Yannikov I.M., Telegin M.V. [Principles for the creation of integrated security systems of critical and potentially dangerous objects]. *Intellektual'nye sistemy v proizvodstve*. 2017. Vol. 15, no. 1. Pp. 105-109 (in Russ.).

3. Nikitin N.A., Ivakhnyuk G.K., Trofimov I.V. [Fundamentals of security at potentially hazardous objects of circulation of petroleum products]. *Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii.* Pp. 27-31. Available at http://vestnik.igps.ru/wp-content/uploads/V53/6.pdf (in Russ.).

4. National standard of the Russian Federation GOST ISO / IEC 31010: 2009. Risk management. Risk assessment methods (in Russ.).

5. Maksimenko V.N., Yasyuk V.E. [The main approaches to the analysis and assessment of information security risks]. *Ekonomika i kachestvo sistem svyazi.* 2017. No. 2. Pp. 42-48 (in Russ.).

6. Hoffman L.D. *Sovremennye metody zashchity informatsii* [Modern methods of information security] (ed. V. A. Gerasimenko). Moscow, Sov. Radio Publ., 1980. 264 p. (in Russ.).

7. Averchenkov V.I., Rytov M.Yu., Gaynullin T.R. [Optimization of the selection of the composition of engineering information protection tools based on the Clements-Hoffman model]. *Vestnik Bryanskogo GTU*. 2008. No. 1. Pp. 61-67 (in Russ.).

8. Rytov M.Yu., Lutsenko I.V. *Realizatsiya sistemy proektirovaniya zashchity dannykh dlya malogo predpriyatiya* [Implementing a data protection design system for a small business]. *Informatsionnaya bezopasnost' i zashchita personal'nykh dannykh. Problemy i puti ikh resheniya* [Proc. Information security and protection of personal data. Problems and solutions: X Interregional Scientific and Practical Conference]. Bryansk, BGTU, 2018. Pp. 151-156. Available at http: konf.x-pdf.ru/19tehnicheskie/213514-1 (accessed 15. 08.2018) (in Russ.).

9. Telegin M.V., Yannikov I.M., Kudelkin V.A., Ushakov I.S. [Models and methods for assessing the safety of critical and potentially dangerous objects]. *Intellektual'nye sistemy v proizvodstve*. 2017. Vol. 15, no. 1. Pp. 118-121 (in Russ.).

* * *

Features of Implementation of the System of Assessing the Security of Critically Important and Potentially Hazardous Objects Based on the Clements-Hofman Method

I. M. Yannikov, DSc in Engineering, Associate Professor, Kalashnikov ISTU, Izhevsk, Russia
M. V. Telegina, PhD in Engineering, Associate Professor, Kalashnikov ISTU, Izhevsk, Russia

The paper assesses the existing approaches to the problem of assessing the security of hazardous facilities. It is proposed to carry out an assessment using the system of modeling and calculating the state of protection of hazardous objects developed on the basis of the Clements-Hoffman method, in which a set of threats, protection mechanisms and objects of protection are used to describe the system of protection with full overlap. This system can be used to calculate any type of protection of hazardous objects when entering data on any threats and appropriate means of protection. The paper provides a block diagram of the security system, a functional diagram, the main parameters and stages of development and testing.

Keywords: critical object, potentially hazardous object, methods of risk analysis and object security, Clements-Hoffman method, full overlap protection system.

Получено: 29.11.18