

Е. В. Бурькова, канд. пед. наук, доц., e-mail: tulpan63@bk.ru,
Оренбургский государственный университет

Программная реализация выбора средств физической защиты объекта информатизации

Рассмотрена задача автоматизированного выбора средств системы физической защиты объекта информатизации. Проведен анализ методов, применяемых для решения данной задачи; проанализированы этапы выбора средств физической защиты, представлена функциональная модель и архитектура программной реализации, разработана программа, реализующая автоматизированный выбор средств защиты.

Ключевые слова: система физической защиты, выбор средств, программная реализация

Введение

Высокий уровень информатизации современного общества обуславливает создание информационно-среды на различных объектах как экономической, так и социально-культурной сферы. Практически все предприятия, организации, частные фирмы представляют собой объекты информатизации, обладающие совокупностью информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средствами их обеспечения. Несанкционированный доступ на объект информатизации может привести к краже либо модификации конфиденциальной информации, краже или порче технических средств хранения, обработки и передачи информации, а также материальных и финансовых средств, и в конечном итоге нанести ущерб объекту, привести к материальным потерям, потере репутации организации и другим ущербам. Угрозы физической безопасности объекта, связанные с проникновением нарушителя и совершением им несанкционированных действий, приводящих к нарушению технологических процессов объекта и всякого рода потерям (людским, материальным, финансовым, информационным), обостряются и модифицируются. В связи с этим проблема создания надежной системы физической защиты объекта

информатизации, решающей задачи обнаружения и предотвращения несанкционированного доступа, является актуальной.

Анализ методов выбора

Система физической защиты — это совокупность инженерно-технических, сигнализационных, программно-аппаратных и иных средств для защиты объектов от хищений, диверсий и других неправомерных действий, позволяющая на заданном уровне осуществлять создание трудностей, ограничение возможностей для нарушителя и увеличение времени проникновения его на объект охраны.

В работах [1, 2] нами были проанализированы основные этапы, выполняемые при проектировании системы физической защиты объекта информатизации. Необходимо выполнить следующую последовательность этапов.

1. Провести обследование объекта.
2. Установить категорию объекта по уровню важности.
3. Составить список требований руководящих документов к физической защите объекта выявленной категории важности.
4. Составить модель угроз и провести оценку рисков физической безопасности.
5. Установить критерии выбора средств физической защиты.

6. Осуществить выбор средств физической защиты.

Необходимо учитывать, что система физической защиты периодически должна подвергаться процедуре проверки эффективности ее функционирования. Это означает, что возникает необходимость проводить оценку уровня защищенности объекта информатизации для выбора рационального состава средств физической защиты, позволяющих снизить риски от потенциальных угроз. Актуальной задачей является разработка программной реализации всех перечисленных выше этапов, что позволит сократить временные затраты и наиболее оптимально выбрать средства физической защиты.

В задаче проектирования системы физической защиты самым сложным и плохо формализуемым этапом, предусматривающим процесс обработки экспертных знаний, является выбор средств физической защиты. Для реализации этой задачи применяют различные методы. Анализ публикаций ученых [3, 5–8, 10], проводивших исследование в данной области, показал, что наиболее часто применимы методы, показанные на рис. 1: это метод анализа иерархий; методы нечеткой логики; логико-вероятностный метод; генетический алгоритм. Рассмотрим кратко эти методы в контексте их применения для решения задачи выбора средств физической защиты.



Рис. 1. Методы выбора средств физической защиты

Генетический алгоритм. Генетические алгоритмы имеют некоторые преимущества перед другими методами, применяемыми при построении систем поддержки принятия решений. Один из таких алгоритмов был рассмотрен в работе [3] и применен авторами при разработке программы проектирования систем физической защиты GenalgSfz. Эффективность работы этих алгоритмов зависит от выбранных параметров: вероятности кроссинговера; вероятности мутаций; числа точек деления хромосом при кроссинговере и др. Чаще всего поиск лучших значений параметров проводится экспериментально. Дополнительная

сложность при определении наилучших значений параметров генетического алгоритма вызывается тем, что необходимо определить не постоянные значения, а правила изменения параметров в процессе поиска решения.

Логико-вероятностный метод. Применение логико-вероятностного подхода применяется для оценки физической защиты объектов и позволяет количественно оценить уровень защищенности путем анализа эффективности средств физической защиты. Данный подход является актуальным, так как определение уровня защищенности и степени рисков позволяет устранить недостатки систем физической защиты, функционирующих на объекте [4]. Этот метод был использован при построении программы анализа физической защищенности объекта *SecurityTips*, главной задачей которой является вычисление степени риска охраняемых зон объекта и выявление наименее защищенной зоны для ее дальнейшей модернизации.

Метод анализа иерархий. При использовании этого метода проводятся парные сравнения средств физической защиты и их способность нейтрализовать актуальные угрозы безопасности. Эксперты определяют вероятность реализации угроз, размер ущерба от реализации каждой угрозы, затем вычисляется риск от каждой угрозы. Риск от угрозы равен нулю, если данное средство защиты нейтрализует угрозу. Для определения относительной вероятности реализации угроз, показателей эффективности средств защиты и коэффициентов затрат на них используют матрицы парных сравнений. Данный метод в применении к решению задачи проектирования систем физической защиты был рассмотрен в работе [6].

Методы нечеткой логики. Эти методы представляют собой математический аппарат работы с объектами, не имеющими жестких, однозначно задаваемых границ. Данная теория позволяет формально описывать нестрогие, нечеткие понятия, формализовано описывать и обрабатывать информацию в случае физической неопределенности и представлять, обрабатывать информацию в случае лингвистической неопределенности. Теория нечетких множеств хорошо согласуется с условиями моделирования систем физической защиты и дает лучшие результаты по сравнению с получаемыми при классических алгоритмах. В качестве множеств рассматриваются следующие: множество элементарных зон защиты объекта; множество

угроз; множество оценок важности зон; множество средств физической защиты; множество оценок эффективности средств защиты; множество оценок стоимости. Между основными множествами устанавливают соответствие. В работе [10] было описано применение метода нечеткой логики и авторы использовали данный метод при разработке программы проектирования состава систем физической защиты *FuzzyConclusion*.

Каждый из рассмотренных методов имеет определенные достоинства и недостатки. Для реализации задачи выбора средств физической защиты необходимо выполнить представленную выше последовательность этапов, при разработке программы был применен логико-вероятностный метод, его формализованное описание было приведено в работе [4].

Функциональная модель и архитектура программы выбора средств физической защиты

Для автоматизации приведенных этапов процесса выбора средств физической защиты была разработана функциональная модель в нотации IDEF0, представленная на рис. 2. Входными данными являются:

- данные для определения категории защищаемого объекта (функционально-отраслевая принадлежность, категория важности, категория защищаемой информации, показатели технической укреплённости и т. д.);
- помеховая обстановка на объекте (наличие ЛЭП, железнодорожных линий, автомо-

бильной трассы и других помех, влияющих на работу охранных извещателей);

- перечень защищаемых ресурсов, оценка их значимости и ценности;
- установленные средства защиты (для учета возможности интеграции новых средств защиты с имеющимися на объекте);
- угрозы физической безопасности.

На основе определения актуальных угроз безопасности строится матрица соответствия угроз и средств защиты для их нейтрализации.

Выходными данными является спецификация средств физической защиты.

Для автоматизации приведенных этапов процесса выбора средств физической защиты была разработана программа, архитектура которой представлена на рис. 3.

Разработанная архитектура состоит из следующих подсистем:

- анализа защищаемого объекта;
- формирования результатов анализа объекта;
- формирования требований к средствам физической защиты;
- выбора средств физической защиты;
- формирования спецификации выбранных средств физической защиты.

Подсистема анализа защищаемого объекта состоит из модулей анализа свойств защищаемого объекта, таких как функционально-отраслевая принадлежность, анализ деятельности объекта, учет числа присутствующего персонала и посетителей, помеховая обстановка вокруг объекта, характеристики техниче-

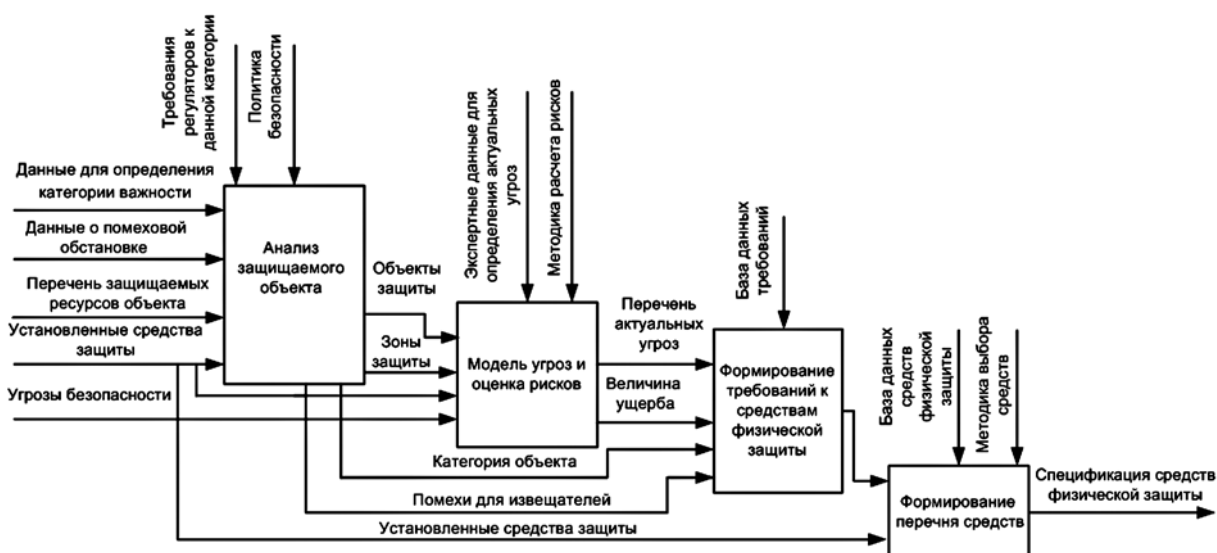


Рис. 2. Функциональная модель процесса выбора средств физической защиты

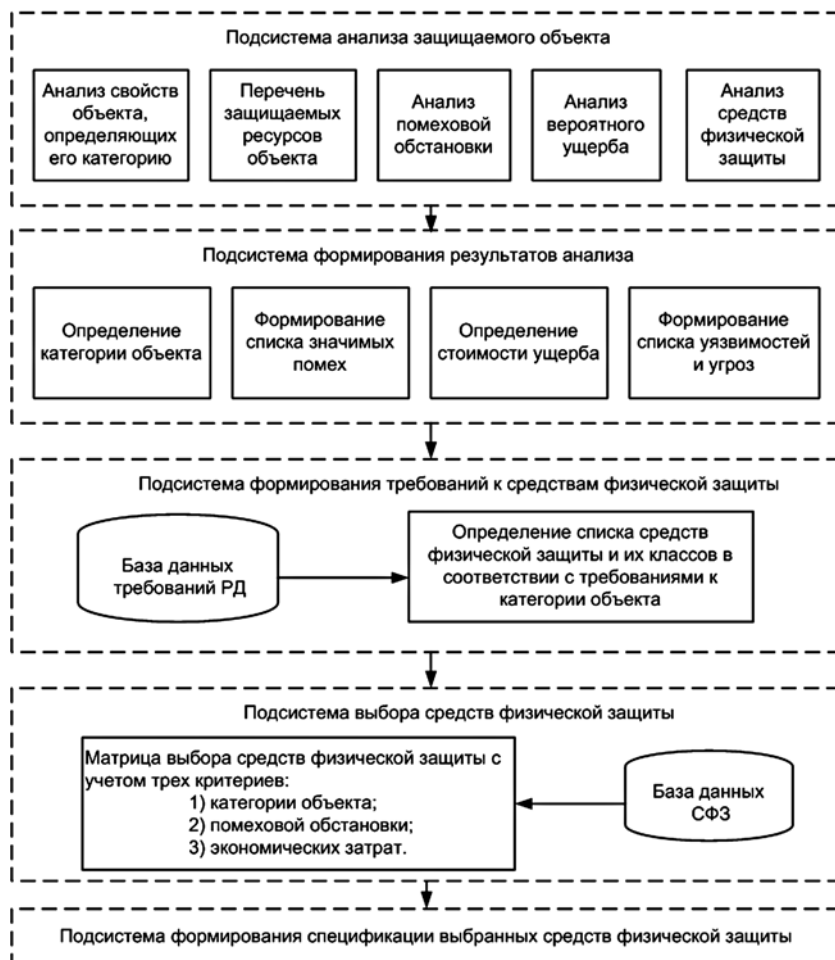


Рис. 3. Архитектура программы

ской укрепленности объекта, учет вероятного ущерба от реализации угроз, учет имеющихся средств физической защиты на объекте.

Подсистема формирования результатов анализа предназначена для получения следующей результирующей информации на основе проведенного обследования объекта: категория по уровню важности; список защищаемых ресурсов; стоимость возможного ущерба; список уязвимостей.

Подсистема формирования требований к средствам физической защиты осуществляет выбор из руководящих документов списка требований, соответствующих категории защищаемого объекта.

Подсистема выбора средств физической защиты осуществляет выбор на основе трех основных критериев: категории объекта; помеховой обстановки; предполагаемых экономических затрат на реализацию системы физической защиты.

Пользовательский интерфейс программы представлен на рис. 4.

Рис. 4. Пользовательский интерфейс программы

На данном этапе программа проходит обследование инженерно-технической укрепленности объекта, вида информационных ресурсов, имеющихся средств защиты, вида защищаемых зон по уровню доступа в них и т. д.

Для каждого этапа процесса выбора реализовано отдельное окно интерфейса. Пользователь программы последовательно проходит все этапы выбора средств защиты, после прохождения каждого этапа формируется результирующий вывод. Например, после этапа обследования объекта формируется таблица результата категорирования объекта.

Результат категорирования объекта

Информативный признак категории	Категория исследуемого объекта
По функционально-отраслевой принадлежности	Объект социально-культурного назначения
По виду возможного ущерба	Людские потери, материальные, финансовые
По масштабу возможного ущерба	Региональный
По важности объекта	Объект категории Б1
По категории информации	Персональные данные, коммерческая тайна
По пожаро- и взрывоопасности	Объект категории Д
По численности персонала свыше 500 человек	Свыше 500 человек
По материальным активам свыше 500 МРОТ	Свыше 500 МРОТ

Разработанная программа предназначена для специалистов по информационной безопасности на защищаемых объектах различного назначения, а также может быть использована в учебном процессе для обучающихся по программам высшего образования по направлению подготовки 10.03.01. Информационная безопасность. Программа была протестирована на трех объектах информатизации. В результате работы программы временные затраты на выбор средств физической защиты были значительно снижены, уровень защищенности объектов соответствовал заявленным требованиям нормативных документов.

Заключение

Задача автоматизированного выбора средств физической защиты является актуальной в условиях современных угроз безопасности объектов информатизации. Автоматизация

информационных процессов позволит обеспечить качество и снизить трудоемкость выполнения данной задачи. Архитектура программы состоит из подсистем, отражающих этапы проведения выбора средств физической защиты и учитывает следующие критерии выбора: категория защищаемого объекта; помеховая обстановка на объекте; экономические затраты на систему физической защиты. Разработанная программа автоматизации выбора средств физической защиты отличается от существующих тем, что охватывает все необходимые этапы решения данной задачи и позволит определить наилучший вариант состава средств физической защиты для обеспечения высокого уровня безопасности объекта с учетом выбранных критериев оптимизации.

Список литературы

1. Бурькова Е. В. Категорирование объектов информатизации для выбора средств физической защиты // Университетский комплекс как региональный центр образования, науки и культуры: материалы Всерос. науч.-метод. конф., Оренбург, 2017. С. 3073—3076.
2. Бурькова Е. В. Структура системы поддержки принятия решений при выборе средств физической защиты // Компьютерная интеграция производства и ИПИ-технологии: материалы VIII Всерос. науч.-практ. конф., Оренбург, 2017. С. 186—189.
3. Шрейдер М. Ю., Боровский А. С., Тарасов А. Д. Проектирование систем физической защиты с помощью генетического алгоритма // Интернет-журнал "Науковедение". 2017. Т. 9, № 4. С. 67.
4. Бурькова Е. В., Гайфулина Д. А., Хакимова Э. Р. Прикладная программа оценки физической защищенности объекта на основе логико-вероятностного подхода // Материалы VI Международной науч.-практ. конф. "Информационные ресурсы и системы в экономике, науке и образовании". Пенза, 2016. С. 10—14.
5. Дураковский А. П., Петров В. Р. Применение математического аппарата при проектировании систем физической защиты // Безопасность информационных технологий. 2012. № 2. С. 80—84.
6. Костин В. Н., Шевченко С. Н., Гарнова Н. В. Проектирование систем физической защиты потенциально опасных объектов на основе развития современных информационных технологий и методов синтеза сложных систем. Оренбург: ИПК "Университет", 2014. 202 с.
7. 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. № 1. С. 105—109.
8. Лукоянов С. В., Белов С. В. Основные требования к системам физической защиты на этапе их проектирования // Вестник Астраханского технического университета. 2010. № 2. С. 163—171.
9. Оладько В. С. Модель выбора рационального состава средств защиты в системе электронной коммерции // Вопросы кибербезопасности. 2016. № 1 (14). С. 17—22.
10. Боровский А. С., Тарасов А. Д. Использование методов нечеткой логики в задачах моделирования процессов // Информационные системы и технологии. 2010. № 3. С. 63—71.

Program Implementation of the Selection of Physical Protection of the Object of Informatization

The purpose of the article is to consider the problem of automated selection of the means of the physical protection system of the informatization object. The analysis of the methods used to solve this problem is carried out; the stages of the choice of means of physical protection are analyzed, the functional model and the architecture of the software implementation are presented, a program is developed that implements the automated selection of protection means.

Keywords: physical protection system, choice of means, software implementation

DOI: 10.17587/it.24.725-730

References

1. Burkova E. V. Kategorirovanie ob#ektov informatizacii dlja vybora sredstv fizicheskoy zashhity (Categorization of informatization objects for the choice of physical protection means), *Universitetskij kompleks kak regional'nyj centr obrazovaniya, nauki i kul'tury: materialy Vseros. nauch.-metod. konf.* Orenburg, 2017, pp. 3073—3076 (in Russian).
2. Burkova E. V. Struktura sistemy podderzhki prinjatija reshenij pri vybere sredstv fizicheskoy zashhity (Structure of the decision support system when choosing the means of physical protection), *Komp'yuternaja integracija proizvodstva i IPI-tehnologii: materialy VIII Vseros. nauch.-prakt. konf.* Orenburg, 2017, pp. 186—189 (in Russian).
3. Shrejder M. Ju., Borovskij A. S., Tarasov A. D. Proektirovanie sistem fizicheskoy zashhity s pomoshh'ju geneticheskogo algoritma (Designing physical protection systems using a genetic algorithm), *Internet-zhurnal "Naukovedenie"*. 2017, vol. 9, no. 4, pp. 67 (in Russian).
4. Burkova E. V., Gajfulina D. A., Hakimova Je. R. Prikladnaja programma ocenki fizicheskoy zashhishhennosti ob#ekta na osnove logiko-verojatnostnogo podhoda (Application program for assessing the physical security of an object on the basis of a logical-probabilistic approach), *Materialy VI Mezh-dunarodnoj nauch.-prakt. konf. "Informacionnye resursy i sistemy v jekonomike, nauke i obrazovanii"*. Penza, 2016, pp. 10—14 (in Russian).
5. Durakovskij A. P., Petrov V. R. Primenenie matematicheskogo apparata pri proektirovanii sistem fizicheskoy zashhity (Usage of Mathematical Apparatus for the Design of Physical Protection Systems), *Bezopasnost' informacionnyh tehnologij*, 2012, no. 2, pp. 80—84 (in Russian).
6. Kostin V. N., Shevchenko S. N., Garnova N. V. Proektirovanie sistem fizicheskoy zashhity potencial'no opasnyh ob#ektov na osnove razvitija sovremennyh informacionnyh tehnologij i metodov sinteza slozhnyh sistem (Designing physical protection systems for potentially dangerous objects on the basis of the development of modern information technologies and methods for the synthesis of complex systems), Orenburg, IPK "Universitet", 2014, 202 p. (in Russian).
7. Kudel'kin V. A., Jannikov I. M., Telegina M. V. Principy sozdaniya integrirovannyh sistem bezopasnosti kriticheski vazhnyh i potencial'no opasnyh ob#ektov (Principles for the creation of integrated security systems for critical and potentially hazardous facilities), *Intellektual'nye sistemy v proizvodstve*, 2017, no. 1, pp. 105—109 (in Russian).
8. Lukojanov S. V., Belov S. V. Osnovnye trebovaniya k sistemam fizicheskoy zashhity na jetape ih proektirovaniya (Basic requirements for physical protection systems at the stage of their design), *Vestnik Astrahanskogo tehničeskogo universiteta*, 2010, no. 2, pp. 163—171 (in Russian).
9. Olad'ko V. S. Model' vybora racional'nogo sostava sredstv zashhity v sisteme jelektronnoj kommercii (Model of the choice of the rational composition of remedies in the electronic commerce system), *Voprosy kiberbezopasnosti*, 2016, no. 1 (14), pp. 17—22 (in Russian).
10. Borovskij A. S., Tarasov A. D. Ispol'zovanie metodov nechetkoj logiki v zadachah modelirovaniya processov (The use of fuzzy logic methods in modeling problems of processes), *Informacionnye sistemy i tehnologii*, 2010, no. 3, pp. 63—71 (in Russian).