УДК 004.056 Вестник УрФО № 2(44) / 2022, с. 30–36

Герасимова К.С., Михайлова У.В., Баранкова И.И. DOI: 10.14529/secur220204

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОПТИМИЗАЦИИ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье рассмотрен подход к оптимизации процесса категорирования объектов критической информационной инфраструктуры (далее – КИИ). Оптимизация процесса реализована за счет разработки программного обеспечения для категорирования объектов КИИ, которое позволит существенно снизить временные затраты на осуществление процесса категорирования. Категорирование выполняется на основании Постановления Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». В статье рассматривается функционал и принцип работы разработанного приложения.

Разработанное программное обеспечение позволяет выполнять оценку категории значимости объекта КИИ на основании исходных данных в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ. В приложении реализована возможность присвоения объекту КИИ одной из категорий значимости или принятие решения об отсутствии необходимости присвоения ему одной из категорий значимости. Результаты категорирования в разработанном приложении оформляются актом, который содержит исходные сведения об объекте КИИ, сведения о присвоенной объекту КИИ категории значимости и необходимый состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости.

Ключевые слова: *информационная безопасность, критическая информационная инфраструктура, объекты критической информационной инфраструктуры, категорирование объектов, разработка программного обеспечения.*

DEVELOPMENT OF SOFTWARE TO OPTIMIZE THE CATEGORIZATION OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

The purpose of this research work is to optimize the process of categorizing objects of critical information infrastructure (hereinafter referred to as CII). To achieve this goal, it was decided to develop software for categorizing CII objects. Categorization is carried out on the basis of Decree of the Government of the Russian Federation of February 8, 2018 No. 127 «On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values». The article discusses the principle of operation of the developed application.

The developed software makes it possible to evaluate the category of significance of the CII object based on the initial data in accordance with the list of indicators of criteria for the significance of the scale of possible consequences in the event of computer incidents at the CII objects. It is possible to assign a CII object to one of the categories of significance, or a decision is made that there is no need to assign one of the categories of significance to it. The categorization results are documented in an act that contains the initial information about the CII object, information about the significance category assigned to the CII object and the necessary set of security measures for a significant object of the corresponding significance category.

Keywords: *information security, critical information infrastructure, critical information infrastructure objects, categorization of objects, software development.*

Категорирование объектов критической информационной инфраструктуры (далее – КИИ) является обязательным с 1 января 2018, когда вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1], регулирующий отношения в области обеспечения безопасности КИИ РФ. Так, субъекты КИИ должны определить категорию значимости для каждого из принадлежащих им объектов КИИ или принять решение об отсутствии необходимости присвоения объекту одной из категорий значимости и предоставить данные во ФСТЭК Россия.

Категорирование – ресурсоемкая работа, предполагающая инвентаризацию всех информационных систем, автоматизированных систем управления и сетей, используемых субъектом КИИ, а также определение категории значимости для каждого такого объекта на основании утвержденных Постановлением Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [2] правил категорирования. У одного субъекта КИИ могут быть сотни таких систем, поэтому категорирование – очень сложный и длительный процесс.

Использование автоматизированной системы значительно упрощает и ускоряет процедуру категорирования, что особенно важ-

но в случаях, когда под контролем субъекта КИИ находится множество объектов КИИ.

Для ускорения и облегчения процесса категорирования разработано программное обеспечение, позволяющее оптимизировать этот процесс. Результатом категорирования является отчет, оформленный согласно требованиям приказа ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» [3].

Среди существующих программных продуктов можно выделить платформу «R-Vision SGRC», разработанную компанией R-Vision, и программный комплекс «Security Vision КИИ», созданный компанией «Интеллектуальная безопасность».

R-Vision SGRC обеспечивает решение следующих задач:

• Ведение реестра активов организации;

• Проведение категоризации объектов КИИ (ведение перечней объектов КИИ и связанных критических процессов, автоматический расчет категории значимости на основе опроса экспертов, формирование пакета документов по результатам категорирования);

• Проведение оценки соответствия активов нормативным и законодательным требованиям;

• Проведение оценки рисков информационной безопасности;

• Ведение базы внутренней документации по информационной безопасности;

• Автоматизация функций по формированию отчетности.

Security Vision КИИ позволяет субъектам КИИ:

• собирать и структурировать всю информацию по объектам КИИ на единой платформе;

• категорировать объекты КИИ согласно законодательству;

• осуществлять непрерывный контроль соответствия защищенности объектов КИИ нормативным требованиям;

• автоматизировать формирование отчетности по форме регулятора.

Преимуществом разработанного приложения перед уже существующими является простота и удобство интерфейса. Так же категорирование можно выполнять либо в ручном режиме, где специалист будет определять значения показателей защищенности, либо в автоматическом, где приложение будет рассчитывать рекомендованные значения показателей защищенности на основе исходных данных. В приложении можно открыть Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» для ознакомления с правилами категорирования объектов КИИ.

Рассмотрим работу разработанной программы «Категорирование объектов КИИ».

При запуске программы открывается главная форма (рис.1).

Перед выполнением категорирования на форме необходимо в верхней половине заполнить все обязательные исходные данные: Наименование объекта, Адрес размещения объекта, Назначение объекта, Сфера деятельности, Архитектура объекта, Площадь и Тип объекта. Также следует заполнить сведения о программных, программно-аппаратных средствах, используемых на объекте КИИ (рис.2).

Следующим шагом необходимо добавить все критические процессы, связанные с объектом КИИ, которые необходимо прокатегорировать [4].

Для автоматического расчета рекомендованных значений показателей значимости необходимо указать будет дополнительные сведения. В случае, если специалист проводит расчет категорий значимости самостоятельно, то для удобства он может воспользоваться «Справочной информацией» и ознакомиться с полным содержанием Постановления Правительства №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изменениями от 24 декабря 2021 г.).

После всей выполненной работы формируются «Акт категорирования объекта критической информационной инфраструктуры», оформленный по требованиям Приказа ФСТЭК и необходимый состав мер по обеспе-

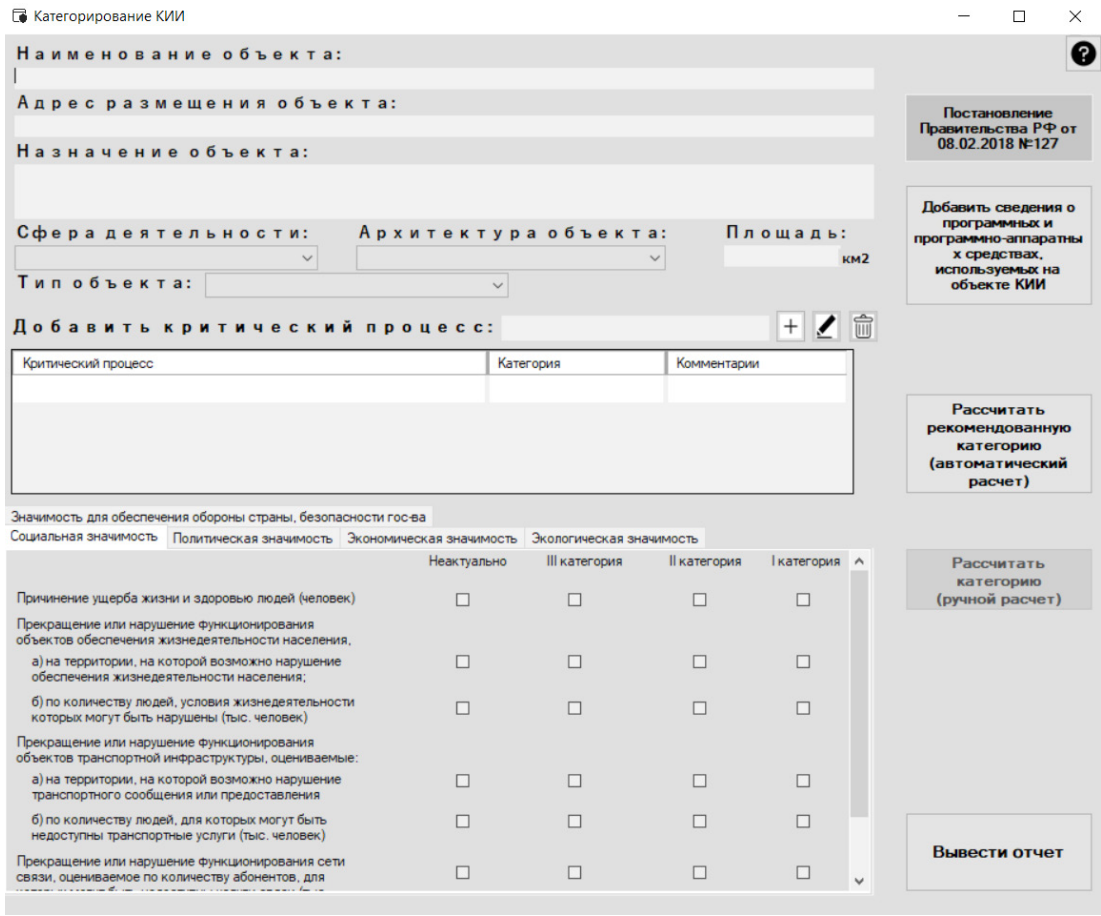

Рис. 1. Главная форма приложения

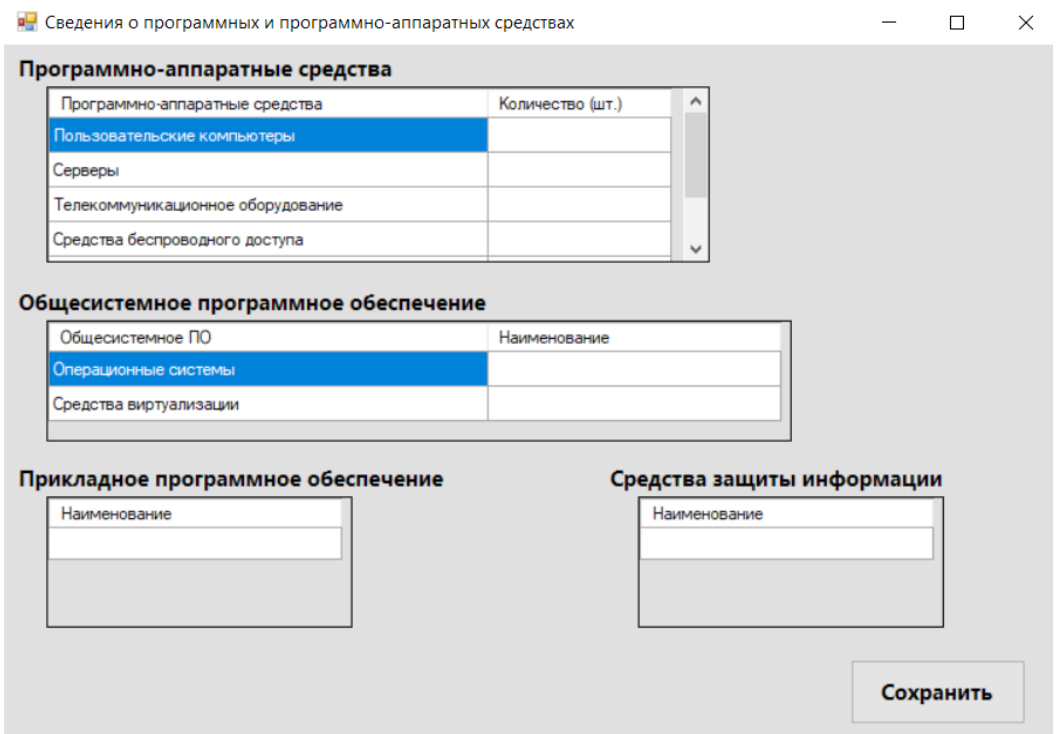

Рис. 2. Форма «Сведения о программных и программно-аппаратных средствах»

чению безопасности для значимого объекта соответствующей категории значимости, сформированный согласно Приказу ФСТЭК России №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [5] (рис.3).

Акт категорирования объекта критической информационной инфраструктуры

УТВЕРЖДАЮ

_____
(руководитель организации)

_____
(подпись, инициалы, фамилия)

«___»_____20___г.

А К Т
категорирования объекта критической информационной инфраструктуры
<NAME>
_____
(наименование объекта)

На основании приказа от «___»_____20___г. №_____комиссия в составе:

председатель комиссии: _____
(роль, должность, фамилия, инициалы)

члены комиссии: _____
(роль, должность, фамилия, инициалы)

_____
(роль, должность, фамилия, инициалы)

_____
(роль, должность, фамилия, инициалы)

в соответствии с требованиями Федерального закона от 26.07.2017 №187, постановления Правительства РФ от 08.02.2018г. №127 провела категорирование объекта критической информационной инфраструктуры <NAME>.
В ходе работы комиссия по категорированию определила:

1. Сведения об объекте критической информационной инфраструктуры (далее – КИИ), представленные в Приложении 1.
2. Сведения об угрозах безопасности информации объекта КИИ, представленные в Приложении 2.
3. Реализованные на объекте КИИ меры по обеспечению безопасности, представленные в Приложении 3.
4. Масштаб возможных последствий в случае возникновения компьютерных инцидентов в соответствии с перечнем показателей критериев значимости, представленный в Приложении 4.

На основании результата анализа значений показателей критериев значимости объекта КИИ в соответствии с постановлением Правительства РФ от 08.02.2018г. №127 объекту <NAME>
_____
(наименование объекта)
присвоена категория<CATEGORY>

Состав необходимых мер по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, утвержденными приказом ФСТЭК от 25.12.2017 № 239, представлен в Приложении 5.

Председатель комиссии: _____
(ФИО, подпись)

Члены комиссии: _____
(ФИО, подпись)

_____
(ФИО, подпись)

_____
(ФИО, подпись)

Приложение 1

Сведения об объекте КИИ:

Наименование объекта	<NAME>
Адреса размещения объекта	<ADDRESS>
Сфера (область) деятельности, в которой функционирует объект	<SCOPE>
Назначение объекта	<APPOINTMENT>
Критические процессы, которые обеспечиваются объектом	<PROCESSES>
Архитектура объекта	<ARCHITECTURE>

Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ:

Программно-аппаратные средства	Пользовательские компьютеры - шт. Серверы - шт. Телекоммуникационное оборудование - шт. Средства беспроводного доступа - шт. Производственное оборудование - шт. Иные программно-аппаратные средства - шт.
Общесистемное программное обеспечение	Наименования операционных систем: Средства виртуализации:
Прикладное программное обеспечение	
Средства защиты информации	

Сведения о взаимодействии объекта КИИ и сетей электросвязи.

Категория сети электросвязи	
Наименование оператора связи	
Цель взаимодействия с сетью электросвязи	
Способ взаимодействия с сетью электросвязи	

Рис. 3. Шаблон Акта категорирования объекта КИИ

Таким образом, было разработано программное обеспечение «Категорирование КИИ» для оптимизации и ускорения процесса категорирования объектов КИИ. Результатом работы и категорирования является отчет «Акт категорирования объекта критической информационной инфраструктуры», содержащий в себе все исходные данные об объекте (Наименование объекта, Адрес размещения объекта, Назначение объекта, Сфера деятельности, Архитектура объекта, Площадь и Тип объекта, Критические процессы, Сведения о программных средствах, программно-аппаратных и средствах защиты информации), перечень показателей критериев значимости и их значения, а так же состав мер по обеспечению безопасности для объекта соответствующей категории значимости.

Литература

1. Федеральный закон №187 «О безопасности критической информационной инфраструктуры Российской Федерации» [Текст], Принят Государственной Думой 12 июля 2017 г., Одобрен Советом Федерации 19 июля 2017 г. – 2017. – 21 с.

2. Постановление Правительства РФ № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [Текст], Принят 8 февраля 2018 г. – 2018. – 20 с.

3. Приказ ФСТЭК России №236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий», Принят 22 декабря 2017 г. – 2017. – 7 с.

4. Баранкова, И.И. О.В. Пермякова. Определение перечня защищаемых ресурсов и их критичности. Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова, 2016. – 14 с.

5. Приказ ФСТЭК России №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Текст], Утвержден ФСТЭК России 25 декабря 2017 г. – 2017. – 37 с.

References

1. Federal'nyy zakon №187 «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» [Tekst], Prinyat Gosudarstvennoy Dumoy 12 iyulya 2017 g., Odobren Sovetom Federatsii 19 iyulya 2017 g. – 2017. – 21 p.

2. Postanovlenie Pravitel'stva RF № 127 «Ob utverzhdenii Pravil kategorirovaniya ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe perechnya pokazateley kriteriev znachimosti ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy» [Tekst], Prinyat 8 fevralya 2018 g. – 2018. – 20 p.

3. Prikaz FSTEK Rossii №236 «Ob utverzhdenii formy napravleniya svedeniy o rezul'tatakh prisvoeniya ob"ektu kriticheskoy informatsionnoy infrastruktury odnoy iz kategoriy znachimosti libo ob otsutstvii neobkhodimosti prisvoeniya emu odnoy iz takikh kategoriy», Prinyat 22 dekabrya 2017 g. – 2017. – 7 p.

4. Barankova, I.I. O.V. Permyakova. Opredelenie perechnya zashchishchaemykh resursov i ikh kritichnosti. Magnitogorsk: Magnitogorskiy gosudarstvennyy tekhnicheskiy universitet im. G.I. Nosova, 2016. – 14 p.

5. Prikaz FSTEK Rossii №239 «Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» [Tekst], Utverzhden FSTEK Rossii 25 dekabrya 2017 g. – 2017. – 37 p.

ГЕРАСИМОВА Ксения Сергеевна, студент 5 курса, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: gierasimovak@mail.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: u.mihaylova@magtu.ru

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

GERASIMOVA Ksenia Sergeevna, student, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: gierasimovak@mail.ru

MIKHAILOVA Uliana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information Security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: u.mihaylova@magtu.ru

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Head of the Department of Informatics and Information Security, Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave., 38. E-mail: inna_barankova@mail.ru