УДК 004.056.5 Вестник УрФО № 4(30) / 2018, с. 75–82

Шабуров А. С., Двойнишников Н. Э., Шлыков А. И. DOI: 10.14529/secur180411

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ПО КАТЕГОРИРОВАНИЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье анализируется последовательность выполнения требований законодательства в области категорирования объектов критической информационной инфраструктуры. На основе рекомендаций сформированы алгоритмы, для каждого этапа выполнения требований. Данные алгоритмы позволяют систематизировать информацию, предоставленную в нормативноправовых актах, а также раскрывают особенности реализации установленных требований. Детально рассмотрены этапы формирования комиссии по категорированию, формирования перечня объектов критической информационной инфраструктуры, а также отдельные этапы категорирования объектов.

Ключевые слова: *критическая информационная инфраструктура, объект критической информационной инфраструктуры, категорирование объектов, защита информации, компьютерная атака.*

Shaburov A. S., Dvoinishnikov N. E., Shlykov A. I.

FEATURES OF THE IMPLEMENTATION OF THE REQUIREMENTS FOR THE CATEGORIZATION OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

The article analyzes the sequence of the requirements of the legislation. The article analyzes the sequence on the implementation of the requirements of legislation in the field of critical information infrastructure of the Russian Federation in terms of categorization of critical information infrastructure objects. Based on the recommendations, algorithms were formed, for each

stage of meeting the requirements separately. These algorithms allow you to systematize the information provided in regulatory legal acts, facilitates its assimilation, and also describes the subtleties of the implementation of the established requirements. The stages of the formation of a commission for categorization, the formation of a list of objects of critical information infrastructure, as well as the actual stage of categorization of objects are considered in detail.

Keywords: *critical information infrastructure, critical information infrastructure facility, categorization of objects, information security, computer attack.*

В современных условиях деятельность по обеспечению безопасности объектов критической информационной инфраструктуры приобретает особую актуальность. В 2018 г. вступил в силу закон «О безопасности критической информационной инфраструктуры Российской Федерации» [1] (далее – 187-ФЗ), открыв новый нормативно определенный перечень требований в сфере информационной безопасности.

В целом, отрасль критической информационной инфраструктуры Российской Федерации (далее – КИИ) концептуально направлена на сферы социально-экономической деятельности, отнесенные к приоритетам устойчивого социально-экономического развития Российской Федерации, а именно: повышение качества жизни российских граждан, экономический рост, наука, технологии, образование здравоохранение и культура, экология и рациональное природопользование[2].

На данный момент проблема реализации требований 187-ФЗ является наиболее широко обсуждаемой кругах специалистов по информационной безопасности в России. Причина столь пристального внимания к данной проблеме состоит, как в отсутствии практического опыта реализации нормативных требований, так и в недостаточной проработанности изданных нормативных документов. Примером может служить неоднозначность определения категории объекта КИИ, в соответствии с «Перечнем показателей критериев значимости объектов критической инфраструктуры Российской Федерации и их значений» [3]. Проблема заключается в том, что показатель 2 и 3 категории объекта КИИ не может быть определен корректно, исходя из определенных границ их значений (рис. 1).

Показатель	Значение показателя		
	III категория	II категория	I категория
9. Возникновение ущерба бюджетам Российской Федерации, оцениваемого:			
а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	более 0,005, но менее или равно 0,1	более 0,1

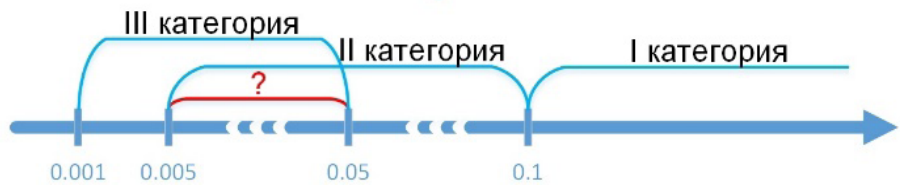

Рис. 1. Неоднозначность толкования категории объекта КИИ

В данной статье, рассматривается лишь часть требований по обеспечению безопасности КИИ, касающуюся категорирования объектов КИИ (далее - Категорирование). Подобный анализ направлен не только на облегчение понимания тонкостей реализации требований нормативных документов, но и на предотвращение ошибок, провоцируемых неоднозначностью толкования отдельных требований. Дальнейшую деятельность целесообразно представить в виде последовательности этапов.

Этап 1. Составление перечня объектов КИИ, подлежащих категорированию. Представляется целесообразным начать работу именно с данного этапа, вопреки поряд-

ку, предлагаемому в [3]. Это обосновано тем, что в комиссию по категорированию (далее - Комиссия) следует включать исключительно тех специалистов, которые в высшей степени осведомлены в особенностях работы объектов КИИ, непосредственно связаны с созданием или обслуживанием объектов КИИ. В противном случае этап категорирования объектов КИИ может сильно затянуться. Практика показывает, что безошибочно определить состав комиссии по категорированию практически невозможно.

В целях исключения возможных ошибок в работе Комиссии по категорированию КИИ, в состав комиссии целесообразно включить уполномоченного в вопросах, касающихся IT-инфраструктуры Организации (чаще всего это главный системный администратор или начальник IT-отдела). Председателя Комиссии необходимо уполномочить в формировании состава Комиссии, а сотрудников организации – в безотлагательной консультативной помощи председателю Комиссии. Формировать Комиссию следует исключительно в процессе составления перечня объектов КИИ, подлежащих категорированию (далее – Перечень объектов), в целях безошибочного определения уровня осведомленности сотрудников.

Чтобы понять процесс составления Перечня объектов КИИ более детально, рассмотрим несколько наиболее характерных вариантов подобных ситуаций:

зиям, которыми обладает организация, а также всем направлениям видов деятельности организации, перечисленных в уставе. После данной процедуры из Перечня исключаются все повторяющиеся процессы.

После составления перечня всех процессов, производимых организацией, выделяются процессы, которые являются критическими. Основное свойство критического процесса заключается в необходимости его выполнения и определяется исходя из последствий его нарушения.

Завершающим шагом на данном этапе является определение процессов, реализуемых за счет информационных систем, информационно-телекоммуникационных сетей и (или) автоматизированных систем управления, принадлежащих Организации. Данные объекты КИИ следует включить в Перечень объектов.

Вариант 2: Организации не характерна высокая степень интеграции вычислительных систем, сетей и средств автоматизации, т. е. количество объектов КИИ не велико.

В данном случае совокупное количество объектов КИИ не должно превышать 10 шт. Тогда можно с легкостью определить, какой объект КИИ отвечает за критический процесс и внести его в Перечень объектов.

Составляя Перечень объектов, стоит учитывать, что распределенный объект КИИ возможно сегментировать (рис. 2). Таким образом, распределенный объект КИИ **С**, включающий в свой состав объекты **А** и **В**, может быть сегментирован на объекты КИИ **А** и **В**, в случае чего в Перечень объектов будут вписаны только объекты **А** и **В**. Для этого должны выполняться следующие требования:

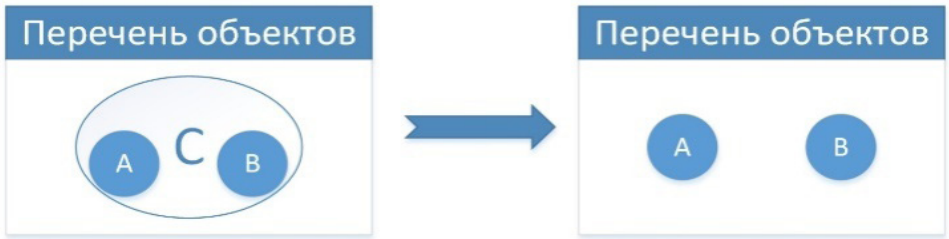

Рис. 2. Сегментирование объектов КИИ

Вариант 1: субъекту КИИ (далее – Организация) характерна высокая степень интеграции вычислительных систем, сетей и средств автоматизации. В данном случае количество объектов КИИ крайне велико, что может спровоцировать ошибки при их перечислении и оставлении Перечня объектов.

Составление Перечня объектов начинается с составления перечня всех процессов, производимых организацией. Для составления данного перечня необходимо обратиться к ОКВЭД, ЕГРЮЛ и уставу организации, лицен-

1. Объект **А** должен быть обособлен программноаппаратно, и, при исключении из объекта **С** этой части, функционирование объекта **В** будет продолжаться планомерно. Иначе говоря, выделяемый объект КИИ должен функционировать автономно.

2. Критические процессы, обеспечивае-

мые выделяемым объектом **А**, не взаимосвязаны с критическими процессами, обеспечиваемыми объектом **В**.

Обобщенный алгоритм формирования состава Перечня объектов КИИ представлен на рис. 3

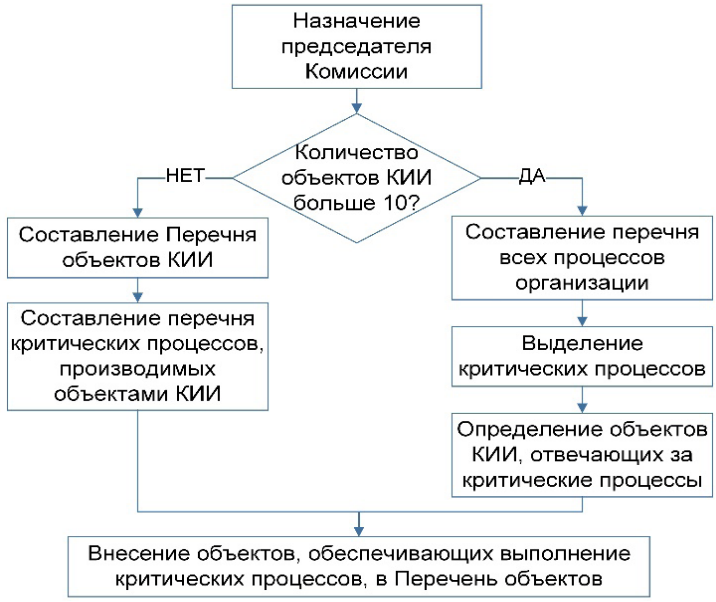

Рис. 3. Алгоритм формирования состава Перечня объектов КИИ

Этап 2. Формирование комиссии по категорированию и заполнение формы перечня объектов КИИ, подлежащих категорированию. По итогу формирования Перечня объектов у председателя Комиссии формируется представление о необходимом составе Комиссии. Ограничения по количественному составу сотрудников, составляющих Комиссию, нет. В то же время, следует минимизировать их количество, с точки зрения экономии временных и человеческих ресурсов. Состав Комиссии формируется исходя из компетентности ее членов в вопросах основных функций и состава программно-аппаратных устройств объектов КИИ, подлежащих категорированию, а также на основании эксплуатационной документации объекта КИИ (приказа на ввод в эксплуатацию, технического задания на разработку и др.).

Рис. 4. Алгоритм формирования Перечня объектов КИИ

В состав Комиссии запрещено включать сотрудников, не связанных с обеспечением безопасности организации, а также не связанных с осуществлением видов деятельности в области информационных технологий. Исключением является руководитель Организации.

В случае, если Организация является подведомственной, то решение включить в состав Комиссии представителя головной организации, уполномоченного в согласовании Перечня объектов с подведомственными организациями, позволит избавиться от необходимости согласовывать Перечень объектов КИИ, что может потребовать дополнительного времени.

Результатом выполнения первых двух этапов по составлению Перечня объектов и работы Комиссии, является формирование информации по составу объектов КИИ [4]. Целесообразно представить ее в табличном варианте (рис.5).

№ п/п	Наименование объекта	Тип объекта	Сфера деятельности, в которой функционирует объект	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество представителя, его телефон, адрес электронной почты

Рис. 5. Форма представления информации по составу КИИ

Этап 3. Категорирование объектов КИИ. Данный этап гораздо более объемный и трудоемкий по сравнению с этапом составления Перечня. В соответствии с требованиями законодательства на Категорирование отводится один год с момента утверждения Перечня объектов. Результатом его выполнения является Акт категорирования объектов КИИ (далее – Акт категорирования), подписанный членами Комиссии и утвержденный руководителем, и заполненная форма [5].

В Акте категорирования должны содержаться следующие сведения:

1. Сведения об объекте КИИ.

2. Результаты анализа угроз безопасности информации объекта КИИ.

3. Реализованные меры по обеспечению безопасности объекта КИИ.

4. Сведения о присвоенной объекту КИИ категории значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий.

5. Сведения о необходимых мерах по обеспечению безопасности [6].

Акт категорирования не имеет стандартной формы, хранится как документ внутреннего пользования и может запрашиваться регулятором во время проверки. Акт категорирования объектов КИИ утверждается руководителем Организации.

Форма направления сведений о результатах присвоения объекту КИИ одной из категорий значимости должна быть утверждена руководителем Организации и отправлена в управление ФСТЭК России в течение десяти дней с момента утверждения Акта категорирования. Данная форма нацелена на комплексное описание объекта КИИ и должна содержать:

1. Сведения об объекте КИИ.

2. Сведения о субъекте КИИ.

3. Сведения о взаимодействии объекта КИИ и сетей электросвязи.

4. Сведения о лице, эксплуатирующем объект КИИ.

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

6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ.

7. Возможные последствия в случае возникновения компьютерных инцидентов.

8. Категория значимости, которая присвоена объекту КИИ.

9. Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта КИИ.

При этом, наиболее существенными для обеспечения информационной безопасности КИИ являются п. 6-9 [7].

Пункт 6 требует формирования модели угроз безопасности информации и модели нарушителя в отношении рассматриваемого объекта КИИ. При их формировании нужно руководствоваться такими документами, как «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» и «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры».

Пункт 7 требует рассмотрения и анализа всех возможных негативных социальных, политических, экономических, экологических последствий и последствий для обороны страны, к которым привело прекращение выполнения критического процесса, за обеспечение которого отвечает рассматриваемый объект КИИ. Для этого требуется проанализировать все показатели критериев значимости объектов КИИ и их значений, к которым приведет прекращение и(или) нарушение работы рассматриваемого объекта КИИ.

Качественная оценка, в первую очередь необходимо:

– проанализировать уязвимости объектов КИИ и характерных инцидентов, связанных с последствиями компьютерных атак на компоненты объектов КИИ;

– рассмотреть потенциальные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации. Если таковые действия невозможны, то это необходимо обосновать;

– провести оценку угроз безопасности информации, в соответствии с перечнем показателей критериев значимости тяжестью возможных последствий, в случае возникновения компьютерных инцидентов на объектах КИИ.

Пункт 8 требует расчета значений тех показателей критериев значимости, которые были выбраны ранее. Расчет производится из соображений о том, что наступили худшие обстоятельства из всех возможных, но в рамках разумного. Иначе говоря, следует найти такую конфигурацию происходящих/не происходящих критических процессов, при которой последствия будут максимально пагубными. При этом, унифицированного метода расчета не предлагается. Руководствоваться при расчете необходимо логикой и здравым смыслом, а значения показателей критериев значимости объекта КИИ напрямую определяют категорию его значимости.

Сначала категория значимости определяется в соответствии с каждым полученным значением показателя критерия значимости в отдельности. Затем из всех полученных критериев выбирается самое высокое значение категории значимости объекта КИИ. Если объект не является значимым (ни одно из значений показателей критериев значимости не достигло даже показателя третьей категории значимости), то категория ему не присваивается.

Пункт 9 требует перечислить все реализованные меры, направленные на обеспечение конфиденциальности, целостности и доступности информации, обрабатываемой категорируемым объектом КИИ. С целью экономии времени будет гораздо более выгодным решением сначала заполнить форму из [5], после чего просто включить сведения из нее в Акт категорирования.

Таким образом, реализация требований по категорированию объектов КИИ и последующая их защита является сложным процессом, включающим комплекс различных задач, требующим итерационного подхода и коллегиальности в принятии решений на каждом из этапов. Пути решения наиболее часто возникающих вопросов являются универсальными, с одной стороны, с другой, - требуют учета характерных особенностей объекта критической инфраструктуры. Качественная реализация требований по категорированию объектов КИИ является основой для обеспечения их информационной безопасности в условиях актуальных угроз безопасности информации.

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26.07.2017. [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

2. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ № 683 от 31.12.2015. [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

3. 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: Постановление Правительства РФ № 127 от 08.02.2018. [Электронный ресурс]: Доступ из справ.правовой системы «КонсультантПлюс».

4. О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации: Информационное сообщение № 240/22/2339 от 04.05.2018. [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

5. 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: Приказ ФСТЭК России № 236 от 22.12.2017. [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России № 239 от 25.12.2017 (ред. от 09.08.2018). [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

7. Борисов С.В. КИИ. Категорирование объектов, часть 1 // SecurityLab.ru: [электронный ресурс] URL: https://www.securitylab.ru/blog/personal/sborisov/344035.php (дата обращения: 24 октября 2018г.).

References

1. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Federal'nyy zakon № 187-FZ ot 26.07.2017. [The law of the Russian Federation # 187-FL from 26.07.2017 "On the Security of the Critical Information Infrastructure of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_220885/ (accessed 2 July 2018)

2. O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii: Ukaz Prezidenta Rossiyskoy Federatsii № 683 ot 31.12.2015. [Presidential Decree # 683 from 31.12.2015 "On the National Security Strategy of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_191669/ (accessed 17 July 2018).

3. Ob utverzhdenii pravil kategorirovaniya ob'yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe perechnya pokazateley pokazateley znachimosti ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy: Postanovleniye Pravitel'stva Rossiyskoy Federatsii № 127 ot 08.02.2018 [Resolution of the Government of the Russian Federation # 127 from 08.02.2018 "On the approval of the rules for categorizing the objects of the critical information infrastructure of the Russian Federation, as well as the list of indicators of the significance indicators of the objects of the critical information infrastructure of the Russian Federation and their values"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_290595/6fd5c84bc2921316798d46fcf3d736b5f223b3c3/ (accessed 2 July 2018).

4. O metodicheskikh dokumentakh po voprosam obespecheniya bezopasnosti informatsii v klyuchevykh sistemakh informatsionnoy infrastruktury Rossiyskoy Federatsii: Informatsionnoye soobshcheniye № 240/22/2339 ot 04.05.2018. [FSTEC Information Communication # 240/22/2339 from 04.05.2018 "On methodological documents on ensuring information security in key information infrastructure systems of the Russian Federation"]. Available at: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1585-informatsionnoe-soobshchenie-fstek-rossii-ot-4-maya-2018-g-n-240-22-2339 (accessed 13 July 2018).

5. Ob utverzhdenii formy napravleniya svedeniy o rezul'tatakh prisvoyeniya ob"yektu kriticheskoy informatsionnoy infrastruktury odnoy iz kategoriy znachimosti libo ob otsutstvii neobkhodimosti prisvoyeniya yemu odnoy iz takikh kategoriy: Prikaz FSTEK Rossii № 236 ot 22.12.2017. [FSTEC Order # 236 from 22.12.2017 "On the approval of the form for sending information on the results of assigning a critical information infrastructure to an object of one of the significance categories or about the absence of the need to assign one of such categories to the object"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_295855/c2b49c620b4a6d35245ddbc52c2bb621252443cb/ (accessed 13 July 2018).

6. Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Prikaz FSTEK Rossii № 239 ot 25.12.2017. [FSTEC Order # 239 from 25.12.2017 "On the Approval of the Requirements for Ensuring the Security of Significant Objects of the Critical Information Infrastructure of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_294287/ (accessed at 27 June 2018).

7. Borisov S.V. KII. Kategorirovaniye obyektov, chast 1 [Borisov S.V. KII. Categorization of objects, part 1]. Available at: https://www.securitylab.ru/blog/personal/sborisov/344035.php (accessed at 24 October 2018).

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент кафедры автоматики и телемеханики. Пермский национальный исследовательский политехнический университет. 614990, г. Пермь, Комсомольский пр., 29. E-mail: shans@at.pstu.ru

ДВОЙНИШНИКОВ Николай Эдуардович, студент кафедры автоматики и телемеханики Пермский национальный исследовательский политехнический университет. 614990, г. Пермь, Комсомольский пр., 29. E-mail: rerfrerf00@gmail.com

ШЛЫКОВ Алексей Игоревич, студент кафедры автоматики и телемеханики Пермский национальный исследовательский политехнический университет. 614990, г. Пермь, Комсомольский пр., 29. E-mail: thekingofthedas@gmail.com

SHABUROV Andrey, Candidate of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. Email: shans@at.pstu.ru

DVOINISHNIKOV Nikolai, student of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. E-mail: rerfrerf00@gmail.com

SHLYKOV Alexey, student of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. E-mail: thekingofthedas@gmail.com