УДК 004.056:656 + 681.518 Вестник УрФО № 1(31) / 2019, с. 48–52

Заведенская А. А., Зырянова Т. Ю.

DOI: 10.14529/secur190107

ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ ТРАНСПОРТА, КАК СУБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В связи с вступившим в силу 1 января 2018 года Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» одной из наиболее актуальных проблем в области информационной безопасности на текущий момент является выполнение требований законодательства по обеспечению безопасности критической информационной инфраструктуры. В статье рассматриваются основные этапы реализации требований Закона для субъектов, функционирующих в транспортной сфере деятельности и являющихся субъектами критической информационной инфраструктуры.

Ключевые слова: *критическая информационная инфраструктура, субъект КИИ, объект КИИ, категорирование объектов, АСУ ТП.*

Zavedenskaya A. A., Zyryanova T. Yu.

MEETING THE REQUIREMENTS FOR INFORMATION SECURITY OF TRANSPORT ENTERPRISES AS SUBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

Federal law № 187 «About security of critical information infrastructure of the Russian Federation» entered into force on 1 January 2018. One of the most urgent problems in the field of information security now is the implementation of the legislation on security of critical information infrastructure. The article examines the main stages of implementation of the requirements of the Law for the entities operating in the transport sector, which are the subjects of critical information infrastructure.

Keywords: *critical information infrastructure, subject CII, object CII categorization of objects, SCADA.*

В связи с вступившим в силу 1 января 2018 года Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» одной из наиболее актуальных проблем в области информационной безопасности на текущий момент является обеспечение безопасности критической информационной инфраструктуры (далее – КИИ) и её защита от компьютерных атак.

Согласно ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1] (далее – Закон о безопасности КИИ):

• КИИ – это совокупность объектов КИИ и сетей, применяемых для их связи.

• Объекты КИИ – информационные системы (ИС), информационно-телекоммуникационные сети (ИТС) и автоматизированные системы управления (АСУ) (более известные как АСУ ТП - АСУ технологическим процессом) субъектов КИИ.

• Субъекты КИИ – лица и (или) индивидуальные предприниматели, которым принадлежат объекты КИИ, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также лица, которые обеспечивают взаимодействие объектов КИИ.

Исходя из этого можно сделать вывод, что организации, функционирующие в транспортной сфере, непосредственно являются субъектами КИИ, а информационные технологии, применяемые, например, для автоматизации процессов, могут оказаться объектами КИИ. Как следствие предприятия транспорта должны обеспечивать выполнение требований Закона о безопасности КИИ.

Рассмотрим основные этапы реализации требований Закона о безопасности КИИ для субъектов транспортной инфраструктуры, являющихся субъектами КИИ.

Первоочередным этапом для субъекта будет проведение категорирования, что является процессом по установлению для объекта КИИ значения по каждому из критериев значимости, в результате которого объекту КИИ присваивается категория значимости, либо выносится решение об отсутствии необходимости присвоения категории. Законодательством определенно три категории значимости – первая, вторая и третья. А критерии значимости делятся на: социальные, политические, экономические, экологические и влияние объекта КИИ на обеспечение обороны страны, безопасности государства и правопорядка.

Подробный процесс проведения категорирования и перечень показателей критериев значимости приведены в Постановлении Правительства РФ от 08.02.2018 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] (далее – Правила).

Для самого проведения категорирования решением руководителя предприятия должна быть созданы комиссия по категорированию, перечень обязательных участников которой представлен в пункте 11 Правил.

Для начала предприятию необходимо произвести первичный сбор данных. На рисунке 1 (с. 50) представлены процессы в рамках первичной подготовки к категорированию и примеры документов, которые могут получиться на выходе.

На самом деле все эти процедуру определены Правилами и законодательно относятся к процессу категорирования, но авторы предлагают вынести это в отдельную первоначальную задачу, т.к. на деле все эти процессы могут оказаться более трудозатратными и требовать участия лиц, не входящих в состав комиссии по категорированию.

Далее переходим непосредственно к самому категорированию (на Рисунке 2 нагляд-

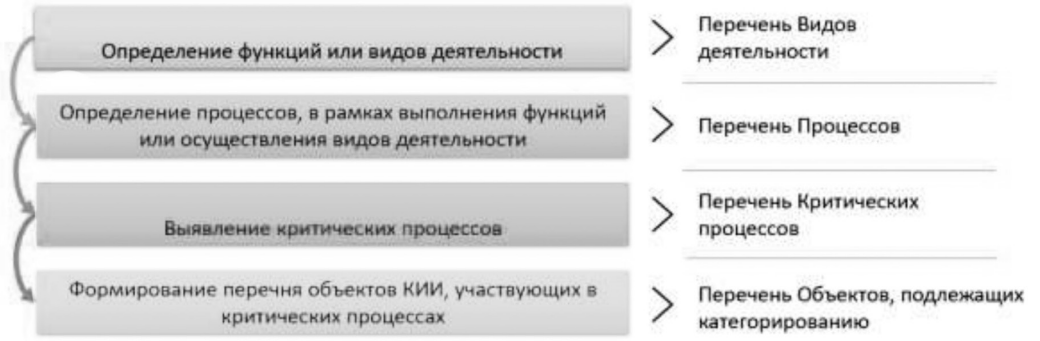

Рис. 1. Первичный сбор данных для категорирования объектов КИИ

Рис. 2. Категорирование объектов КИИ

но представлен процесс проведения категорирования).

Комиссией по категорированию создаётся конечный вариант перечня объектов КИИ, подлежащих категорированию, который должен быть утверждён самим субъектом КИИ. Здесь нужно обратить внимание, что дата утверждения перечня объектов КИИ будет являться своего рода «датой отсчёта» для последующих процессов. Потому что максимальной срок проведения категорирования (равен 1 году) отсчитывается именно с момента утверждения перечня объектов КИИ. Так же и обязательная отправка перечня объектов КИИ, подлежащих категорированию, в орган исполнительной власти, а именно во ФСТЭК России, должна быть произведена в течении 5 рабочих дней с момента его утверждения. Рекомендованную форму перечня объектов КИИ для направления во ФСТЭК России можно найти в Информационном сообщении ФСТЭК России от 24 августа 2018 г. № 240/25/3752.

Обязательный анализ угроз информационной безопасности в ходе проведения категорирования авторы рекомендуют производить посредством разработки базовой модели угроз и дальнейшим созданием частной модели угроз для каждой из систем. При этом базовые модели угроз для АСУ ТП и ИС, например, должны быты разработаны отдельно друг от друга. Согласно Информационному сообщению ФСТЭК России от 4 мая 2018 г. №240/22/2339 при моделировании угроз безопасности информации можно использовать Базовую модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденную ФСТЭК России 18 мая 2007 г., а также Методику определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденную ФСТЭК России 18 мая 2007 г. Но рядом экспертов отмечается, что методики для ключевых систем информационной инфраструкту-

ры в большинстве своём являются устаревшими, и стоит руководствоваться Банком данных угроз, который ведёт ФСТЭК России, и Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

По результатам категорирования оформляются акты и сведения о присвоении объекту КИИ одной из категорий значимости или об отсутствии необходимости присвоения категории. Акт категорирования объектов КИИ должен быть утверждён руководителем предприятия транспорта и является внутренним документом. А сведения заполняются по форме, утвержденной приказом 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» и в течении 10 дней направляются во ФСТЭК России. Так же важным является факт того, что для каждого объекта КИИ должен быть оформлен отдельный акт и сведения, т.е. каждая ИС, ИТС или АСУ ТП, обеспечивающая критические процессы транспортного предприятия, должна иметь свой акт категорирования и по каждой во ФСТЭК России должны быть направлены сведения, независимо от присвоенной категории или от решения об отсутствии необходимости её присвоения.

По решению Коллегии ФСТЭК России от 24 апреля 2018 г. №59 перечень объектов КИИ нужно было создать до 1 августа 2018 года, а категорирование объектов КИИ произвести до 1 января 2019 г.

После проведения категорирования происходит некоторая развилка в ходе действий по выполнению требований Закона о безопасности КИИ, а именно на значимые объекты и на объекты, которым по результатам категорирования категория не была присвоена. На субъекты, у которых значимых объектов КИИ нет, возлагаются обязанности по выполнению ч.2, ст.9 Закона о безопасности КИИ. А для субъектов КИИ со значимыми объектами КИИ к обязанностям ч.2, ст.9 добавляются обязанности ч.3, ст.9 Закона о безопасности КИИ.

Защита значимых объектов КИИ должна производиться согласно Приказу ФСТЭК России от 22 декабря 2017 г. №235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования» и Приказу ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». А вот если объект «не значимый», то обеспечение безопасности можно произвести согласно требованиям Приказа ФСТЭК России от 14 марта 2014 г. №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», но это уже управленческое решение владельца АСУ ТП.

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ: принят Гос. Думой 12 июля 2017 г.: одобр. Советом Федерации 19 июля 2017 г. // СПС Консультант Плюс

2. 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» // Официальный интернет-портал правовой информации (www.pravo.gov.ru) от 13.02.2018 г.; Собрание законодательства Российской Федерации от 2018 г., № 8, ст. 1204

References

1. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: feder. zakon Ros. Federatsii ot 26 iyulya 2017 g. № 187-FZ: prinyat Gos. Dumoy 12 iyulya 2017 g.: odobr. Sovetom Federatsii 19 iyulya 2017 g. // SPS Konsul'tant Plyus

2. Postanovlenie Pravitel'stva RF ot 8 fevralya 2018 g. № 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» // Ofitsial'nyy internet-portal pravovoy informatsii (www.pravo.gov.ru) ot 13.02.2018 g.; Sobranie zakonodatel'stva Rossiyskoy Federatsii ot 2018 g., № 8, st. 1204

ЗАВЕДЕНСКАЯ Анастасия Андреевна, студентка 4 курса электротехнического факультета по направлению подготовки Информационная безопасность Уральского государственного университета путей сообщения, 620034 Екатеринбург, ул. Колмогорова, 66. E-mail: nastyazavedenskaya@yandex.ru

ЗЫРЯНОВА Татьяна Юрьевна, заведующий кафедрой «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, кандидат технических наук. 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: tzyryanova@usurt.ru

ZAVEDENSKAYA Anastasia, 4-year student of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: nastyazavedenskaya@yandex.ru

ZYRYANOVA Tatiana, associate professor of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: tzyryanova@usurt.ru