Татьяна М. Каннер
ЗАО «ОКБ САПР»,
2-й Кожевнический пер., 12, Москва, 115114, Россия
e-mail: tatianash@okbsapr.ru, https://orcid.org/0000-0002-3210-2090

ОСОБЕННОСТИ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2019.2.02

Аннотация. В статье рассматривается программа повышения квалификации, позволяющая слушателям получить знания и навыки в области обеспечения безопасности критической информационной инфраструктуры (КИИ). Программа разъясняет действия государственных органов, учреждений и других организаций при реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Целью статьи является описание особенностей реализации предлагаемой программы повышения квалификации. Приводится состав программы, формы проведения, типы занятий, состав итоговой аттестации, типы документов о прохождении повышения квалификации. Описываются особенности требований к образованию слушателей, поступающих на обучение, а также особенности преподавания программы и взаимодействия со слушателями в рамках курса. Особое внимание уделяется содержащимся в программе практическим вопросам, связанным с организацией защищенной сетевой коммуникации между элементами критической информационной инфраструктуры с применением микрокомпьютеров «m-TrusT». В результате успешного освоения программы слушатели получают удостоверения установленного образца, применяя полученную на курсе информацию, могут организовывать работы по категорированию своих объектов КИИ и реализации требований ФЗ №187 к ним.

Ключевые слова: критические информационные инфраструктуры, КИИ, повышение квалификации по технической защите информации, повышение квалификации в области обеспечения безопасности КИИ, микрокомпьютер «m-TrusT».

Для цитирования: КАННЕР, Татьяна М. ОСОБЕННОСТИ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 22-31, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1214>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.02.

Tatiana M. Kanner
"OKB SAPR",
2nd Kozhevnichesky lane, 12, Moscow,115114, Russia
e-mail: tatianash@okbsapr.ru, https://orcid.org/0000-0002-3210-2090

Features of advanced training of specialists in ensuring safety of significant objects of critical information infrastructure

DOI: http://dx.doi.org/10.26583/bit.2019.2.02

Abstract. The article considers the program of professional development that allows to gain the necessary knowledge and abilities in the field of safety of the critical information infrastructure (CII). This program explains actions of public authorities, institutions and other organizations for fulfilling the requirements of the Federal law of July 26, 2017 No. 187 "About safety of critical information infrastructure of the Russian Federation". The purpose of the article is to describe the features of implementation of the offered program for advanced training. The structure of the program, the form and types of advanced training, structure of the final assessment, types of qualification documents are given. The article also

describes the educational requirements for students entering and features of teaching the program and interaction with students within a course. Special attention is paid to the practical issues contained in the program related to the organization of secure network communication between elements of the critical information infrastructure using “m-TrusT” microcomputers. As a result of successful mastering of the program, students receive standard certificates and with information obtained on the course could organize works on categorization of the objects of the CII’s and fulfill the requirements of Federal Law No. 187 for them.

Keywords: critical information infrastructure, CII, advanced training in the field of technical information security, advanced training in the field of ensuring safety for CII, “m-TrusT” microcomputers.

For citation: KANNER, Tatiana M. Features of advanced training of specialists in ensuring safety of significant objects of critical information infrastructure. IT Security (Russia), [S.l.], v. 26, n. 3, p. 22-31, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1214>. Date accessed: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.02.

Введение

В настоящее время все большую актуальность набирает необходимость получения дополнительного профессионального образования в области критических информационных инфраструктур (КИИ) путем повышения квалификации по данному направлению. Это связано с вступлением в силу 1 января 2018 г. Федерального закона (ФЗ) от 26 июля 2017 г. ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [1]. Данный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (РФ) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

В приведенном законе к объектам КИИ отнесены [1]:

- информационные системы;
- информационно-телекоммуникационные сети;
- автоматизированные системы управления технологическим процессом субъектов КИИ.

А к субъектам отнесены государственные органы, государственные учреждения, российские юридические лица и/или индивидуальные предприниматели, которым на правах собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в 13 сферах: здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности, химической промышленности, а также – российские юридические лица и/или индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [1].

В рассматриваемом ФЗ №187 действия субъектов КИИ относительно их объектов описаны достаточно подробно. Также в настоящее время издан ряд дополняющих данный закон нормативных документов, которые уточняют все требуемые действия. При этом необходимо отметить, что для большинства организаций КИИ, приведенные в данных документах действия, представляются трудными для внедрения в процесс обеспечения безопасности своих объектов критических информационных инфраструктур. Например, в соответствии с требованиями закона, субъекты КИИ должны определить относятся ли их объекты к объектам КИИ, после чего сообщить об этом во ФСТЭК России. Это значит, что субъекты КИИ должны либо присвоить одну из категорий значимости своим объектам, либо не присвоить ни одну из категорий, если объект КИИ не соответствует

критериям значимости. Используемые для этого правила категорирования объектов КИИ утвержденны постановлением Правительства РФ от 8 февраля 2018 года №127 [2]. Данные правила позволяют провести категорирование объектов КИИ. Однако в этих правилах множество различных показателей определения категории, что усложняет выбор правильного варианта [3].

Помимо этого, в соответствии с данным ФЗ необходимо интегрироваться в ГосСОПКА – государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. В законе не приводятся действия субъектов КИИ по обеспечению встраивания в ГосСОПКА. Эту информацию можно получить из приказов ФСБ России №367 и №368 от 24 июля 2018 г. [4, 5], регламентирующих перечень и порядок предоставления информации субъектами КИИ в ГосСОПКА, а также порядки обмена информацией о компьютерных инцидентах субъектами КИИ (в том числе иностранными учреждениями и организациями) и получения ими информации о средствах и способах проведения компьютерных атак и методах их предупреждения и обнаружения. Однако данные документы содержат множество специализированных нюансов, доступных только специалистам в области обеспечения безопасности КИИ [3].

Также, следуя закону ФЗ №187, субъекты КИИ должны соблюдать требования по обеспечению безопасности значимых объектов КИИ, утвержденные Приказом ФСТЭК России от 21 декабря 2017 г. №235 [6]. В требованиях рассматриваются этапы обеспечения безопасности значимых объектов КИИ, включающие планирование, разработку, реализацию необходимых мероприятий, контроль состояния и совершенствование их безопасности. Несмотря на то, что данные требования достаточно конкретные, начинающему специалисту в области КИИ сложно определить, например, какие именно средства защиты подходят для его системы. Понимание данных вопросов можно приобрести путем изучения примеров различных объектов КИИ, разбора требований к их средствам обеспечения безопасности и выбора конкретного средства защиты в каждом случае.

Из рассмотренного выше видно, что большинству субъектов критических информационных инфраструктур, даже после изучения соответствующих приказов и постановлений, в связи с наличием множества вопросов будет достаточно сложно самостоятельно провести категорирование объектов КИИ, организовать работы по интеграции в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ и обеспечению безопасности объектов КИИ в соответствии с требованиями федерального закона №187. Получить соответствующие знания, навыки и умения, которые могут ответить на все эти вопросы, позволяет прохождение курса повышения квалификации в области обеспечения безопасности критических информационных инфраструктур [3].

В связи с этим ОКБ САПР совместно с Московским физико-техническим институтом (МФТИ) реализует программу повышения квалификации «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры».

В данной статье рассматриваются особенности предлагаемой программы повышения квалификации специалистов по обеспечению безопасности значимых объектов КИИ, связанные с ее реализацией в соответствии с требованиями ФСТЭК России к программам повышения квалификации, а также с приобретением дополнительных компетенций, необходимых при реализации этих требований на реальных объектах критических информационных инфраструктур.

Основная часть

Одной из важных особенностей реализации предлагаемой «ОКБ САПР» совместно с МФТИ программы повышения квалификации является ее разработка в соответствии с «Методическими рекомендациями по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации», утвержденными ФСТЭК России 16 апреля 2018 г., и примерной программой повышения квалификации «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры», утвержденной ФСТЭК России 17 декабря 2018 г. Разработка программы в соответствии с приведенными документами от ФСТЭК означает, что все положения, модули и темы программы утверждены регуляторами и соответствуют законодательству РФ. Поэтому полученные в рамках курса знания могут быть на законном основании применены субъектами КИИ для реализации требований ФЗ №187 в действительности.

Помимо этого, следует обратить внимание на особенность, связанную с необходимостью планового/внепланового прохождения курсов повышения квалификации. Слушатели могут пройти обучение при появлении потребности совершенствования или получения новых компетенций в области обеспечения безопасности КИИ, или при плановом повышении квалификации специалистов, ответственных за обеспечение технической защиты информации. Необходимость планового повышения квалификации через определенный период, как известно, связана с правилами, приведенными в постановлении Правительства РФ от 6 мая 2016 г. №399 «Правила организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса» [7]. В соотвествии с данными правилами все федеральные государственные органы, органы государственной власти субъектов РФ, органам местного самоуправления, организациям с государственным участием и организациям оборонно-промышленного комплекса должны проходить повышение квалификации через определенный период времени.

Перед подачей заявки на зачисление на курс необходимо обратить внимание на немаловажную особенность проведения программы – достаточно высокие требования к квалификации поступающих на курс слушателей. Предполагается обучение только тех специалистов, которые имеют высшее образование или диплом о профессиональной переподготовке в области информационной безопасности. Однако это оправдано, так как для освоения рассматриваемого в программе материала они уже должны обладать базовыми знаниями в области информационной безопасности. В этом случае при успешном завершении курса слушатели получают удостоверение МФТИ установленного образца о повышении квалификации в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. При этом необходимо отметить, что слушатель, не имеющий требуемого образования, также может пройти обучение, но под свою персональную ответственность, так как в процессе обучения, не обладая требуемыми знаниями в области информационной безопасности, он должен будет получить их самостоятельно с целью понимания преподаваемого материала. В этом случае по завершении обучения слушатели получают справку с подтверждением прохождения курса, а не удостоверение как слушатели с требуемым образованием.

Еще одной важной особенностью реализации рассматриваемой программы повышения квалификации является ее состав. Предлагаемая программа включает три базовых модуля, рассматривающих основы обеспечения безопасности значимых объектов КИИ, организацию работ по обеспечению безопасности значимого объекта КИИ и контроль за обеспечением безопасности значимого объекта КИИ. При этом в состав программы также входит четвертый специализированный модуль. В этом модуле рассматривается организация защищенной сетевой коммуникации между элементами КИИ с применением разработанных «ОКБ САПР» микрокомпьютеров «m-Trust» [8, 9] – одноплатных компьютеров Новой гарвардской архитектуры [10, 11]. Данный модуль включает большое количество практических и лабораторных работ, что позволит слушателям ознакомиться и научиться применять указанные средства защиты информации (СЗИ) для организации защищенной сетевой коммуникации своих объектов КИИ.

В рамках четвертого модуля рассматривается понятие резидентного компонента безопасности (РКБ) [12, 13], идея которого заложена в «m-Trust». Разбираются ключевые характеристики РКБ, применение РКБ для обеспечения доверенной загрузки операционной системы средства вычислительной техники [14], реализации криптографических алгоритмов (шифрование и подпись), защищенного хранения неизвлекаемых криптографических ключей, ведения неперезаписываемых журналов событий [15, 16], генерации случайных последовательностей. Рассматривается понятие интеграционной платформы «МК-И». Описываются типовые характеристики и параметры микрокомпьютеров «m-TrusT». Приводятся варианты интерфейсных плат, позволяющих коммутировать микрокомпьютер «m-TrusT» в «разрыв» между подконтрольными объектами различного назначения и каналом связи. Большое внимание уделяется особенностям построения защищенной сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT», а также разбираются примеры построения такой коммуникации.

Наличие данного модуля дает возможность слушателям в результате освоения рассматриваемой программы повышения квалификации приобрести новые компетенции, связанные с применением микрокомпьютеров «m-TrusT» для организации защищенного сетевого взаимодействия между элементами КИИ. Такие компетенции являются дополнительными к базовым, определенным в одноименной примерной программе, утвержденной ФСТЭК России, и получаемым в ходе обучения на первых трех модулях рассматриваемой программы. Так, в рассматриваемой программе повышения квалификации к базовым компетенциям добавляются следующие:

а) к общепрофессиональным – способность пользоваться документацией на микрокомпьютеры «m-TrusT»;

б) к профессиональным:

- в организационно-управленческой деятельности:

– способность планировать и разрабатывать мероприятия по обеспечению безопасности сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT»;

– способность реализовывать (внедрять) мероприятия по организации защищенной сетевой коммуникации между элементами КИИ при помощи микрокомпьютеров «m-TrusT»;

- в проектной деятельности – способность разрабатывать предложения по построению защищенной сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT»;

- в эксплуатационной деятельности – способность устанавливать, настраивать и осуществлять администрирование микрокомпьютерами «m-TrusT».

При этом в результате освоения данной программы повышения квалификации, обучающиеся должны получить знания, умения и навыки, также являющиеся дополнительными к базовым, определенным в одноименной примерной программе.

Освоившие четвертый модуль должны:

а) знать:

– основы понятия резидентного компонента безопасности: концепцию корректного старта и путь ее развития в истории эволюции средств вычислительной техники и средств защиты информации;

– характеристики и возможности резидентного компонента безопасности;

– характеристики, особенности настройки и применения микрокомпьютеров «m-TrusT»;

– характеристики интерфейсных плат для подключения микрокомпьютеров «m-TrusT» к различным подконтрольным объектам и каналообразующей аппаратуре;

– особенности построения защищенной сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT»;

– примеры построения защищенной сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT»;

– особенности работы и обновления ключевой системы микрокомпьютеров «m-TrusT»;

б) уметь:

– определять тип необходимой для конкретного подконтрольного объекта и каналообразующей аппаратуры интерфейсной платы подключения микрокомпьютера «m-TrusT»;

– определять необходимый в конкретной ситуации состав программного обеспечения активной части «m-TrusT»;

– применять микрокомпьютеры «m-TrusT» для построения защищенной сетевой коммуникации между элементами КИИ;

– работать с ключевой системой «m-TrusT» и уметь ее обновлять;

в) владеть навыками установки, настройки и применения микрокомпьютеров «m-TrusT» для обеспечения защищенного сетевого взаимодействия между элементами КИИ.

Первые три модуля программы обеспечивают формирование базового уровня знаний, умений, навыков и компетенций у слушателей, необходимых им для профессиональной деятельности в области обеспечения безопасности значимых объектов КИИ. Однако в базовых модулях уделяется внимание обеспечению безопасности объектов КИИ в общем, без рассмотрения конкретных средств защиты, которые можно применять для данной цели. Четвертый модуль включает ряд семинаров, практических и лабораторных занятий, позволяющих познакомиться со средством защиты сетевого взаимодействия между элементами КИИ (микрокомпьютером «m-TrusT») в действительности и получить практический опыт его применения. За счет этого приобретаемые на курсе знания, навыки и умения позволяют слушателям получить всестороннее представление об обеспечении безопасности значимых объектов КИИ в целом, а также освоить практическую сторону данного вопроса. Тем самым наличие дополнительного, четвертого модуля в программе позволяет обеспечить полноту компетенций, необходимых слушателям в области обеспечения безопасности значимых объектов КИИ.

Особенностью реализации программы также является наличие различных форм ее проведения. В базовом варианте рассматриваемая программа построена по очно-заочному принципу с применением электронного обучения и дистанционных образовательных технологий.

Взаимодействие со слушателями по теоретическим вопросам курса (лекции, занятия в режиме круглого стола) осуществляется дистанционно с помощью системы управления образовательным процессом на базе Moodle (СДО – система дистанционного образования). Как правило, при проведении обучения лекции чередуются с занятиями в режиме круглого стола – в конце каждой лекции преподаватель выдает самостоятельные задания (изучить литературу/написать небольшой реферат на одну из тем лекций или вообще на не затронутую на лекции тему/решить какую-то задачу/выполнить какие-либо практические действия), а на занятиях в режиме круглого стола проверяет выполнение задания, отвечает на возникшие вопросы, обсуждает ошибки, особенности, правильное решение и тому подобное.

Взаимодействие со слушателями курса по практическим вопросам курса (семинары, практические занятия, лабораторные работы) осуществляется в виде аудиторных занятий. Аудиторные занятия проходят в рамках нескольких очных сессий, которые, как правило, назначаются на длинные выходные, выпадающие на праздничные дни (например, на новогодние каникулы или праздники в феврале, марте или мае). На таких занятиях преподаватель в том числе демонстрирует рассматриваемые в рамках курса СЗИ на практике и предоставляет возможность поработать с ними самостоятельно, отвечает на возникшие вопросы и помогает решить поставленные задачи.

При отсутствии возможности принять участие в очной сессии слушатели могут проходить практические и лабораторные занятия удаленно, под контролем преподавателя. Для этого «ОКБ САПР» заранее выдает слушателям во временное пользование все необходимое для участия в занятиях программное обеспечение и оборудование. На очных занятиях такие слушатели присутствуют удаленно (через Skype) и принимают в них полноценное участие.

Важно отметить, что как при заочном взаимодействии во время лекций и занятий в режиме круглого стола, так и при вынужденном удаленном выполнении практических и лабораторных работ возможности взаимодействия слушателя и преподавателя достаточно хорошо приближены к очной форме, так как при использовании системы дистанционного обучения слушатели видят преподавателя, использующего веб-камеру, на своих экранах, слышат – через гарнитуру, могут задавать вопросы как голосом (при наличии аналогичной гарнитуры), так и письменно в специально предназначенном для этого в СДО форуме. Для проведения занятий преподаватели могут использовать:

– презентации;

– электронную доску (писать маркером на белом электронном листе, аналогично тому, как это можно сделать в графическом редакторе рисунков);

– белый лист бумаги с дополнительной веб-камерой, транслирующей в реальном времени то, что пишет преподаватель на этом листе при помощи обычной ручки или карандаша (как замена магнитно-маркерной доски);

– предоставление слушателям общего доступа к компьютеру преподавателя («расшаривание» рабочего стола) для демонстрации практической части занятий.

Описанная форма проведения занятий предполагает обучение слушателей без отрыва от основной работы. Однако при необходимости, по желанию организации, возможно проведение очного обучения, с полным отрывом слушателей от работы – очная форма обучения. В этом случае сократится длительность обучения, и слушатели освоят

программу за более короткий срок. Как видно из вышеописанного, слушатели могут принять участие в обучении в любой удобной для них форме.

По завершении занятий «ОКБ САПР», вне зависимости от выбранной формы проведения занятий, выполняет итоговое тестирование слушателей по изученному материалу. В случае успешного прохождения итогового тестирования, слушатели, как уже было указано выше, получают удостоверение МФТИ установленного образца о повышении квалификации в области обеспечения безопасности значимых объектов критической информационной инфраструктуры (либо справку о прохождении курса, при отсутствии требуемого образования).

Заключение

Предлагаемая «ОКБ САПР» совместно с МФТИ Программа повышения квалификации «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры» разработана в соответствии с официальными требованиями ФСТЭК России, изложенными в методических рекомендациях по разработке программ повышения квалификации и соответствующей примерной программой повышения квалификации. То есть в содержании программе разбираются все требования ФЗ №187 и все дополняющие его нормативные документы, а ее положения, модули и темы утверждены ФСТЭК России. Поэтому полученные на курсе знания позволяют субъектам КИИ применять их для своих объектов КИИ без колебаний относительно корректности с точки зрения регулятора.

Программа содержит высокие требования к квалификации поступающих на курс слушателей – они должны иметь высшее образование или диплом о профессиональной переподготовке в области информационной безопасности. В результате обучения после успешного прохождения итогового тестирования слушатели получают удостоверение МФТИ установленного образца. Слушатели, не имеющие такого образования, также могут пройти обучение и итоговое тестирование, но без получения такого удостоверения (выдается справка с подтверждением прохождения курса).

Предлагаемая программа включает четыре модуля, три базовых с основными знаниями в области безопасности КИИ и один специализированный. Последний в основном состоит из практических и лабораторных работ, позволяющих научиться организовывать и обеспечивать защищенные сетевые коммуникации объектов КИИ с применением микрокомпьютеров «m-TrusT» производства «ОКБ САПР». Наличие такого модуля дает возможность слушателям в результате освоения рассматриваемой программы повышения квалификации помимо базовых также приобрести новые знания, умения и навыки и получить новые компетенции, связанные с применением микрокомпьютеров «m-TrusT» для организации защищенного сетевого взаимодействия между элементами КИИ. В связи с этим в результате обучения слушатели получают всестороннее представление об обеспечении безопасности значимых объектов КИИ в целом, в том числе и практической стороне данного вопроса.

При реализации программы предусмотрено несколько форм ее проведения (очно-заочная, очная). При очно-заочной форме возможно удаленное прохождение практических и лабораторных занятий. Слушатели в зависимости от наличия/отсутствия возможности и желания полного отрыва от работы могут принять участие в обучении в любой удобной для них форме.

Подводя итог статьи, необходимо отметить, что актуальность рассматриваемой программы основана на необходимости повышения квалификации в области безопасности

критических информационных инфраструктур, понятие которых появилось в РФ совсем недавно при вступлении в силу Федерального закона № 187-ФЗ. Предлагаемая программа повышения квалификации позволяет получить как базовые, так и дополнительные знания, навыки и умения в области обеспечения безопасности критической информационной инфраструктуры, подтвержденные удостоверением МФТИ установленного образца. А на основании полученной на курсе информации – организовать работы по категорированию своих объектов КИИ и реализации требований ФЗ №187 к ним.

СПИСОКЛИТЕРАТУРЫ:

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ// Государственная дума. 2017. – 20 с.
2. 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 Российской Федерации от 8 февраля 2018 г. №127 // Правительство Российской Федерации. 2018. – 11 с.
3. Каннер Т.М. Повышение квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры // Материалы XXIV научно-практической конференции «Комплексная защита информации», Витебск: ВГТУ, 21–23 мая, 2019. С. 186–191.
4. Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА: Приказ ФСБ Российской Федерации от 24 июля 2018 г. №367 // ФСБ Российской Федерации. 2018. – 10 с.
5. Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения: Приказ ФСБ Российской Федерации от 24 июля 2018 г. №368 // ФСБ Российской Федерации. 2018. – 7 с.
6. Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: Приказ ФСТЭК России от 21 декабря 2017 г. № 235 // ФСТЭК России. 2017. – 10 с.
7. Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса: Постановление Правительства Российской Федерации от 06 мая 2016 г. №399 // Правительство Российской Федерации. 2016. – 2 с.
8. Конявская С.В. Защищенные сетевые коммуникации не требуют «зоопарка» // Национальный банковский журнал. 2018. № 10. С. 92–93.
9. Конявская С.В. Защита сетевой коммуникации: «зоопарк» с человеческим лицом // Инсайд. Защита информации. 2018. № 5. С. 38–41.
10. Конявский В.А. Иммунитет как результат эволюции ЭВМ // Инсайд. Защита информации. 2017. № 4. С. 46–52.
11. Конявский В.А., Конявская С.В. Доверенные информационные технологии: от архитектуры к системам и средствам. Москва: URSS, 2019. – 264 с.
12. Конявский В.А. Доверенные системы как средство противодействия киберугрозам. Базовые понятия // Information Security/Информационная безопасность. 2016. № 3. С. 40–41.
13. Алтухов А.А. Неатомарный взгляд на РКБ как на композицию перехвата управления и контроля целостности // Материалы XX научно-практической конференции «Комплексная защита информации», Минск, 19–21 мая, 2015. С. 53–55.
14. Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: Радио и связь, 1999. – 325 с.
15. Конявская С.В. Неперезаписываемый журнал событий: лайфхак для аудитора // Information Security/Информационная безопасность. 2018. № 1. С. 37.
16. Андреев В.М., Давыдов А.Н. Безопасное хранение журналов работы СЗИ // Материалы XX научно-практической конференции «Комплексная защита информации», Минск, 19 – 21 мая, 2015. С. 49–52.

REFERENCES:

[1] O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii: Federal'nyj zakon ot 26 ijulja 2017 № 187-FZ. Gosudarstvennaja duma. 2017. – 20 s. (in Russian).

[2] Ob utverzhdenii Pravil kategorirovanija ob#ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii, a takzhe perechnja pokazatelej kriteriev znachimosti ob#ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i ih znachenij: Postanovlenie Pravitel'stva Rossijskoj Federacii ot 8 fevralja 2018 g. №127. Pravitel'stvo Rossijskoj Federacii. 2018. – 11 s. (in Russian).

[3] Kanner T.M. Povyshenie kvalifikacii specialistov, rabotayushchih v oblasti obespecheniya bezopasnosti znachimyh ob'ektov kriticheskoj informacionnoj infrastruktury [Professional development of the expert working in the field of security of significant objects of critical information infrastructure]. Materialy XXIV nauchno-prakticheskoj konferencii «Kompleksnaya zashchita informacii», Vitebsk: VGTU, 21–23 maya, 2019 [Proceedings of the scientific and practical conference "Complex Information Security", Vitebsk: VGTU, 21–23 May 2019]. Vitebsk, 2019. S. 186–191 (in Russian).

[4] Ob utverzhdenii Perechnja informacii, predstavljaemoj v GosSOPKA i Porjadka predstavlenija informacii v GosSOPKA: Prikaz FSB Rossijskoj Federacii ot 24 ijulja 2018 g. №367 FSB Rossijskoj Federacii. 2018. – 10 s. (in Russian).

[5] Ob utverzhdenii Porjadka obmena informaciej o komp'juternyh incidentah i Porjadka poluchenija sub#ektami KII informacii o sredstvah i sposobah provedenija komp'juternyh atak i o metodah ih preduprezhdenija i obnaruzhenija: Prikaz FSB Rossijskoj Federacii ot 24 ijulja 2018 g. №368. FSB Rossijskoj Federacii. 2018. – 7 s. (in Russian).

[6] Ob utverzhdenii trebovanij k sozdaniju sistem bezopasnosti znachimyh ob#ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i obespecheniju ih funkcionirovanija: Prikaz FSTJeK Rossii ot 21 dekabrja 2017 g. № 235. FSTJeK Rossii. 2017. – 10 s. (in Russian).

[7] Ob organizacii povyshenija kvalifikacii specialistov po zashhite informacii i dolzhnostnyh lic, otvetstvennyh za organizaciju zashhity informacii v organah gosudarstvennoj vlasti, organah mestnogo samoupravlenija, organizacijah s gosudarstvennym uchastiem i organizacijah oboronno-promyshlennogo kompleksa: Postanovlenie Pravitel'stva Rossijskoj Federacii ot 06 maja 2016 g. №399. Pravitel'stvo Rossijskoj Federacii. 2016. – 2 s. (in Russian).

[8] Konyavskaya S.V. The protected network communications do not demand "zoo". Nacional'nyj bankovskij zhurnal [The National bank magazine]. 2018, n. 10. S. 92–93 (in Russian).

[9] Konyavskaya S.V. Protection of network communication: "zoo" with a human face. Insajd. Zashhita informacii [Insider. Information security], 2018, n. 5. S. 38–41 (in Russian).

[10] Konyavskiy V. A. Immunity as result of evolution of the COMPUTER. Insajd. Zashhita informacii [Insider. Information security], 2017, n. 4. S. 46–52 (in Russian).

[11] Konyavskiy V.A., Konyavskaya S.V. The entrusted information technologies: from architecture to systems and tools. Moscow: URSS, 2019. – 264 s. (in Russian).

[12] Konyavskiy V.A. The entrusted systems as tools of counteraction to cyberthreats. Basic concepts. Information Security. 2016, n. 3. S. 40–41 (in Russian).

[13] Altukhov A.A. Neatomarnyj vzgljad na RKB kak na kompoziciju perehvata upravlenija i kontrolja celostnosti [Not atomic view of a SRC as on composition of interception of management and control of integrity]. Materialy XX nauchno-prakticheskoj konferencii «Kompleksnaja zashhita informacii», Minsk, 19–21 maya 2015 [Proceedings of the scientific and practical conference "Complex Information Security", Minsk 19–21 May 2015]. Minsk, 2015. S. 53–55 (in Russian).

[14] Konyavskiy V.A. Upravlenie zashhitoj informacii na baze SZI NSD «Akkord» [Management of information security on the basis of Accord-TSHM]. Moscow, Radio i svjaz' [Radio and communication], 1999. – 325 s. (in Russian).

[15] Konyavskaya S.V. Not re-recorded log: life hack for the auditor. Information Security. 2018. n. 1. P. 37 (in Russian).

[16] Andreev V.M. Davidov V.M. Bezopasnoe hranenie zhurnalov raboty SZI [Safe storage of DST work logs]. Materialy XX nauchno-prakticheskoj konferencii «Kompleksnaja zashhita informacii», Minsk, 19–21 maya 2015 [Proceedings of the scientific and practical conference "Complex Information Security", Minsk 19–21 May 2015]. Minsk, 2015. P. 49–52 (in Russian).

Поступила в редакцию – 10 июня 2019 г. Окончательный вариант – 16 августа 2019 г.
Received – June 10, 2019. The final version – August 16, 2019.