Для служебного пользования
Экз. № 1

Автономная некоммерческая организация
дополнительного профессионального образования
«Учебный центр «Информзащита»

СОГЛАСОВАНО	УТВЕРЖДАЮ
Начальник Управления ФСТЭК России	Директор АНО ДПО «Учебный центр «Информзащита»
_____ / Мартинец Н.М. *(подпись)*	_____ / Степаненко А.А. / *(подпись)*
«___» _____ 2019 г.	«___» _____ 2019 г.
М.П.	*М.П.*

ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ»

Сокращенное наименование: **«ОБ ЗО КИИ»**

Код: ПК187

Москва
2019

Выписка из Программы повышения квалификации

Полный текст Программы имеет пометку «Для служебного пользования».

Предоставление копии Программы осуществляется только по письменному запросу в соответствии с положениями Постановления Правительства РФ от 03.11.1994 N 1233.

1. Общие положения

Настоящая программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры (далее - Программа повышения квалификации), разработана с учетом положений:

Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

Указа Президента Российской Федерации от 21 февраля 2019 г. № 68 «О профессиональном развитии государственных гражданских служащих Российской Федерации»;

приказа Министерства образования и науки Российской Федерации от 01 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

приказа Министерства образования и науки Российской Федерации от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»;

профессионального стандарта «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 01 ноября 2016 г. № 599н;

профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н;

профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н.

Программа повышения квалификации разработана на основе примерной программы повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, утвержденной ФСТЭК России 30 ноября 2018 г., и 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.

Программа повышения квалификации реализуется в Автономной некоммерческой организации дополнительного профессионального образования «Учебный центр «Информзащита» (АНО ДПО «Учебный центр «Информзащита»), г. Москва.

Программа повышения квалификации разработана в инициативном порядке на основании Приказа Директора АНО ДПО «Учебный центр «Информзащита» от 15 января 2019 г. №03/01/19.

Разработчики Программы повышения квалификации:

- Ершов Дмитрий Вячеславович, кандидат технических наук, заместитель директора по учебно-методической работе;
- Журавлев Владимир Владимирович, заведующий кафедрой юридических проблем

защиты конфиденциальной информации;

- Нугаев Рашид Рустамович, преподаватель отдела обучения.

Программа повышения квалификации обсуждена и одобрена на заседании Методического совета АНО ДПО «Учебный центр «Информзащита» и утверждена Директором Учебного центра 21 июня 2019 г.

2. Цель реализации Программы повышения квалификации

Целью реализации Программы повышения квалификации является совершенствование компетенций, необходимых для осуществления профессиональной деятельности, повышение профессионального уровня в рамках имеющейся квалификации специалистов, в том числе государственных гражданских служащих и муниципальных служащих, субъектов критической информационной инфраструктуры (КИИ) Российской Федерации, ответственных за обеспечение безопасности значимых объектов КИИ.

Обучающиеся по программе повышения квалификации готовятся к осуществлению следующих видов профессиональной деятельности: организационно-управленческая, проектная, эксплуатационная.

Объектами профессиональной деятельности обучающихся являются:

- объекты КИИ - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы субъектов КИИ;
- угрозы безопасности информации, обрабатываемой объектами КИИ;
- способы и средства, используемые для обеспечения безопасности значимых объектов КИИ;
- система нормативных правовых актов, методических документов и национальных стандартов в области обеспечения безопасности значимых объектов КИИ.

Задачами профессиональной деятельности специалистов, работающих в области обеспечения безопасности значимых объектов КИИ, являются:

а) <u>в организационно-управленческой деятельности:</u>

- планирование и разработка мероприятий по обеспечению безопасности значимых объектов КИИ;
- реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов КИИ;
- контроль состояния безопасности значимых объектов КИИ;
- совершенствование безопасности значимых объектов КИИ;

б) <u>в проектной деятельности:</u>

- формирование требований к силам обеспечения безопасности значимых объектов КИИ, к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ, к организационно-распорядительным документам по безопасности значимы объектов КИИ;
- разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению безопасности значимых объектов КИИ;
- проведение анализа угроз безопасности информации в отношении значимых объектов КИИ и выявление уязвимости в них;
- проведение оценки соответствия значимых объектов КИИ требованиям по безопасности;

- подготовка предложений по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов КИИ;

в) в эксплуатационной деятельности:

- планирование мероприятий по обеспечению безопасности значимого объекта КИИ;
- анализ угроз безопасности информации в значимом объекте КИИ и последствий от их реализации;
- управление (администрирование) подсистемой безопасности значимого объекта КИИ;
- управление конфигурацией значимого объекта КИИ и его подсистемой безопасности;
- реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ;
- информирование и обучение персонала значимого объекта КИИ;
- контроль за обеспечением безопасности значимого объекта КИИ.

3. Требования к квалификации поступающего на обучение

К освоению Программы допускаются лица, имеющие высшее образование по направлению подготовки (специальности) в области информационной безопасности, или прошедшие профессиональную переподготовку для выполнения нового вида профессиональной деятельности в области информационной безопасности, подтвержденное документом об образовании.

4. Планируемые результаты обучения

Процесс освоения слушателями Программы повышения квалификации направлен на совершенствование и (или) получение следующих компетенций:

а) общепрофессиональных:

- способность использовать нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ в своей профессиональной деятельности;
- способность использовать достижения науки и техники, пользоваться реферативными и справочно-информационными изданиями в области обеспечения безопасности значимых объектов КИИ;

б) профессиональных:

в организационно-управленческой деятельности

- способность планировать и разрабатывать мероприятия по обеспечению безопасности значимых объектов КИИ;
- способность реализовывать (внедрять) мероприятия по обеспечению безопасности значимых объектов КИИ;
- способность проводить контроль состояния безопасности значимых объектов КИИ;
- способность совершенствовать систему безопасности значимых объектов КИИ;

в проектной деятельности

- способность формировать требования к программным и программно аппаратным средствам, применяемым для обеспечения безопасности значимы; объектов КИИ, к организационно-распорядительным документам по безопасности значимых объектов КИИ;
- способность разрабатывать предложения по совершенствованию организационно-распорядительных документов по обеспечению безопасности значимых объектов

КИИ;

- способность проводить анализ угроз безопасности информации в отношении значимых объектов КИИ;
- способность проводить оценку соответствия значимых объектов КИИ требованиям безопасности;
- способность разрабатывать предложения по совершенствованию функционирования системы безопасности, а также по повышению уровня безопасности значимых объектов КИИ;
- способность выявлять наличие критических процессов у субъекта КИИ;
- способность выявлять объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
- способность формировать перечень объектов КИИ, подлежащих категорированию;
- способность определять категории значимости объектов КИИ;
- способность разрабатывать акт категорирования объекта КИИ и подготавливать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;
- способность осуществлять выбор организационных и технических мер, применяемых для обеспечения безопасности значимого объекта КИИ;

в эксплуатационной деятельности:

- способность планировать мероприятия по обеспечению безопасности значимого объекта КИИ;
- способность анализировать угрозы безопасности информации в значимом объекте КИИ и возможные последствия от их реализации;
- способность управлять (администрировать) системой безопасности значимого объекта КИИ;
- способность управлять конфигурацией значимого объекта КИИ и его системой безопасности;
- способность реагировать на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ;
- способность информировать и обучать персонал значимого объекта КИИ;
- способность проводить контроль за обеспечением безопасности значимого объекта КИИ.

В результате освоения программы повышения квалификации обучающиеся должны получить знания, умения и навыки, которые позволят качественно изменить соответствующие компетенции или получить новые.

Освоившие программу должны:

а) знать:

- нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ;
- основы функционирования государственной системы обнаружения предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

- основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ;
- принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования;
- процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ;
- процедуру подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;
- основные принципы выявления наличия критических процессов у субъекта КИИ;
- основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
- процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ;
- общие требования по обеспечению безопасности значимых объектов КИИ;
- общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования;
- требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ;
- требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ;
- порядок обмена и предоставления информации в рамках государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
- цели, задачи, основные принципы организации государственной контроля в области обеспечения безопасности значимых объектов КИИ;
- порядок обработки результатов контроля (проверки) состояние безопасности значимых объектов КИИ;

б) уметь:

- определять категории значимости объектов КИИ;
- формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоении ему одной из таких категорий;
- выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации;
- обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ;
- определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер в рамках системы безопасности значимого объекта КИИ;
- определять структуру системы безопасности значимого объекта КИИ;
- осуществлять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и программно аппаратными

средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта КИИ;

- определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации;
- определять требования к обеспечению безопасности значимого объекта КИИ;
- организовывать передачу информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) владеть навыками:

- работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объектов КИИ;
- работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами;
- разработки организационно-распорядительных документов по безопасности значимых объектов КИИ;
- эксплуатации системы безопасности значимого объекта КИИ;
- выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ;
- участия в разработке организационных и технических мероприятий по защите объектов КИИ;
- установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ;
- проведения работ по контролю состояния безопасности объектов КИИ.

5. Условия реализации Программы повышения квалификации

На базе АНО ДПО «Учебный центр «Информзащита» развернуты учебные классы, оснащенные персональными компьютерами с комплектом лицензионного программного обеспечения, сертифицированными программными и аппаратными средствами защиты информации, которая позволяет эффективно осваивать практическую часть рабочего материала данной Программы повышения квалификации.

Формирование профессиональных компетенций обеспечивается широким использованием в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В рамках Программы повышения квалификации проведение практических занятий осуществляется специалистами высшего уровня квалификации в области информационной безопасности, имеющими практический опыт работы в российских компаниях и государственных организациях.

Программа повышения квалификации предусматривает проведение занятий в соответствии с целевыми установками Программы повышения квалификации, которые

обеспечивают требуемый уровень усвоения учебного материала. Знания приобретаются на лекциях, семинарах и в ходе самостоятельной работы. Умения и навыки формируются проведением ряда взаимосвязанных практических занятий (лабораторных работ), компьютерного моделирования последствий принимаемых решений, деловых и ролевых игр, разбором конкретных ситуаций, тренингов и др.

Каждому обучающемуся обеспечивается доступ к библиотечному фонду, укомплектованному печатными и электронными изданиями основной учебной литературы, из расчета не менее одного печатного экземпляра на четыре-пять обучающихся.

В фонд дополнительной литературы, помимо учебников, включены официальные, справочно-библиографические и специализированные периодические издания, в том числе правовые нормативные акты и нормативные методические документы в области обеспечения безопасности значимых объектов КИИ в расчете один-два экземпляра на каждые 20 обучающихся.

Обучающимся обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам по тематике информационной безопасности.

Передача Программы повышения квалификации другой образовательной организации не предусматривается.

Внесение изменений в Программу повышения квалификации осуществляется в соответствии с требованиями, установленными законодательными и иными нормативными правовыми актами Российской Федерации в области образования и порядком обращения со служебной информацией ограниченного распространения.

6. Формы аттестации

Итоговая аттестация обучающихся по Программе повышения квалификации – экзамен в форме тестирования.

Перечень тестов, используемых для проведения экзамена, формируется на основе перечней тестов, выносимых для контроля знаний обучающихся при проведении промежуточных аттестаций по учебным модулям (дисциплинам), представленным в рабочей программе курса повышения квалификации.

Для проведения итоговой аттестации создается аттестационная комиссия, состав которой утверждается директором АНО ДПО «Учебный центр «Информзащита».

В целях обеспечения объективного определения теоретической и практической подготовленности обучающихся к выполнению профессиональных задач по результатам обучения в состав аттестационной комиссии могут включаться представители ФСТЭК России, Управления ФСТЭК России по Центральному федеральному округу.

Обучающимся, успешно освоившим Программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

7. Учебный план Программы повышения квалификации

7.1 Категория обучающихся: специалисты (в том числе государственные гражданские служащие) субъектов КИИ, ответственные за обеспечение безопасности значимых объектов КИИ.

7.2 Форма обучения: очная (с отрывом от работы).

7.3 Продолжительность обучения по данной Программе повышения квалификации составляет не менее 108 часов, включая 78 часов всех видов учебных аудиторных занятий, 2 часа зачётов и 28 часов самостоятельной работы обучающихся.

7.4 Режим занятий: 8 академических часов учебных занятий с преподавателем и 2,5 часа самостоятельной работы в день.

7.5 План учебного процесса

№ п/п	Наименование учебных модулей, тем	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	11
1.	**Учебный модуль № 1. Основы обеспечения безопасности значимых объектов КИИ**	**22**	**16**	**6**	**6**	**4**	**-**	**-**	**6**	Текущий контроль. Тестирование
1.1.	Тема № 1. Правовые основы обеспечения безопасности КИИ Российской Федерации	11	8	4	4	-	-	-	3	
1.2.	Тема № 2 Угрозы безопасности информации, обрабатываемой на объектах КИИ	11	8	2	2	4	-	-	3	
2.	**Учебный модуль № 2. Организация работ по обеспечению безопасности значимого объекта КИИ**	**55**	**40**	**11**	**7**	**22**	**-**	**-**	**15**	Текущий контроль. Тестирование
2.1.	Тема № 1. Категорирование объектов КИИ	14	10	4	-	6	-	-	4	
2.2.	Тема № 2. Требования по обеспечению безопасности значимых объектов КИИ	24	18	4	4	10	-	-	6	
2.3.	Тема № 3. Система безопасности значимого объекта КИИ	6	4	2	2	-	-	-	2	
2.4.	Тема № 4. Стадии (этапы) работ по созданию систем безопасности	11	8	1	1	6	-	-	3	
3.	**Учебный модуль № 3. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ**	**11**	**8**	**4**	**4**	**-**	**-**	**-**	**3**	Текущий контроль. Тестирование

1	2	3	4	5	6	7	8	9	10	11
3.1.	Тема № 1. Варианты подключения значимого объекта КИИ к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак.	5	4	2	2	-	-	-	1	
3.2.	Тема № 2. Взаимодействие значимого объекта КИИ с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак.	6	4	2	2	-	-	-	2	
4.	**Учебный модуль № 4. Контроль за обеспечением безопасности значимого объекта КИИ**	**16**	**14**	**4**	**2**	**4**	**4**	**-**	**2**	Текущий контроль. Тестирование
4.1.	Тема № 1. Контроль за обеспечением безопасности значимого объекта КИИ	16	14	4	2	4	4	-	2	
5.	**Итоговая аттестация**	**4**	**2**	**-**	**-**	**2**	**-**	**-**	**2**	Экзамен в форме тестирования
Итого:		**108**	**80**	25	19	32	4	–	**28**	**-**

7.6 Сводные данные по бюджету времени

Общий объем времени, отводимого на освоение программы (календарных дней/часов)			Распределение учебного времени (количество часов)					
Всего	Из них		Всего часов учебных занятий	В том числе		Время на самостоятельную работу	Итоговая аттестация	Резерв учебного времени
	Выходные, праздничные дни	Учебное время		Учебные занятия по расписанию	Практики			
12	2	108	108	80	-	28	Экзамен	-

8. Календарный учебный график

Обучение по Программе повышения квалификации может осуществляться как единовременно (непрерывно), так и в 2 этапа (в порядке, определенном договором на обучение и индивидуальным планом-графиком освоения Программы повышения квалификации). Общее нормативное время освоения Программы повышения квалификации 10 учебных дней (2 недели). Продолжительность обучения: 108 часов.

Срок обучения по Программе повышения квалификации, недели	1	2	
Виды занятий, предусмотренные Программой повышения квалификации	А	А	И

А - аудиторная и самостоятельная работа;
И - итоговая аттестация.