Инструкция по выполнению требований законодательства Российской Федерации о защите критической информационной инфраструктуры организациями, осуществляющими деятельность в сфере оборонной, металлургической и химической промышленности

1. Организациям, подведомственным или находящимся в сфере ведения Минпромторга России, не завершившим работу по определению наличия объектов критической информационной инфраструктуры и их категорированию:

1.1. Создать постоянно действующую комиссию по категорированию в соответствии с требованиями пункта 11 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127[1] (далее – Правила категорирования объектов критической информационной инфраструктуры).

1.2. Провести инвентаризацию всех информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, которые на праве собственности, аренды или на ином законном основании принадлежат организации.

1.3. Провести работу по определению наличия объектов критической информационной инфраструктуры с учётом всех имеющихся в организации информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, в том числе таких как:

локальные вычислительные сети;

информационные системы, предназначенные для разработки и хранения конструкторской документации;

испытательные стенды;

лабораторное оборудование;

системы цифрового моделирования;

информационные системы управления хозяйственной деятельностью, реализующие функции стратегического планирования (BPM-системы, OLAP-системы);

информационные системы управления ресурсами, позволяющие осуществлять планирование, учет, контроль и анализ ресурсов (EPR-системы);

информационные системы, обеспечивающие управлением жизненным циклом продукции (PLM-системы);

информационные системы управления производственными ресурсами в ходе технологического процесса (MES-системы);

---

[1] С изменениями, утверждёнными постановлениями Правительства Российской Федерации от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127», от 24 декабря 2021 г. № 2431«О внесении изменений в постановление Правительства Российской Федерации»

автоматизированные системы, обеспечивающие контроль и (или) управление технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными на нем технологическими и (или) производственными процессами (SCADA-системы, распределенные системы управления);

информационные (автоматизированные) системы управления станками с числовым программным управлением.

1.4. При наличии в организации указанных систем сформировать перечень объектов критической информационной инфраструктуры, подлежащих категорированию, и в соответствии с пунктом 15 Правил категорирования объектов критической информационной инфраструктуры согласовать с:

Департаментом цифровых технологий Министерства промышленности и торговли Российской Федерации (только подведомственным Минпромторгу России организациям);

головными организациями интегрированных структур (организациям, входящим в состав интегрированных структур).

1.5. Направить в ФСТЭК России согласованный и утвержденный перечень объектов критической информационной инфраструктуры, подлежащих категорированию, в соответствии с пунктом 15 Правил категорирования объектов критической информационной инфраструктуры в печатном и электронном виде.

Срок направления: в течение 5 рабочих дней после утверждения перечня.

1.6. Направить в ФСТЭК России сведения о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий, в соответствии с пунктом 5 статьи 7 Федерального закона № 187-ФЗ и пунктом 18 Правил категорирования объектов критической информационной инфраструктуры в печатном и электронном виде по форме, утверждённой приказом ФСТЭК России от 22 декабря 2017 г. № 236, в порядке, установленном информационным сообщением ФСТЭК России от 17 апреля 2020 г. № 240/84/611.

1.7. Направить результаты выполнения решений, изложенных в пунктах № 1 – 5, по форме № 1 (образец формы прилагается) в печатном и электронном виде на оптическом диске в:

ФГУП «НПП «ГАММА» – подведомственные Минпромторгу России организации и головные организации интегрированных структур в сфере ведения Минпромторга России;

Срок направления: до 1 июля 2022 г.

головные организации интегрированных структур – организации, входящие в состав интегрированных структур.

Срок направления: до 1 июня 2022 г.

1.8. Для вновь создаваемых и проектируемых информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем

управления выполнять требования пунктов 8, 18 Правил категорирования объектов критической информационной инфраструктуры.

При этом сведения о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий направляются в ФСТЭК России в печатном и электронном виде по форме, утверждённой приказом ФСТЭК России от 22 декабря 2017 г. № 236 в порядке, установленном информационным сообщением ФСТЭК России от 17 апреля 2020 г. N 240/84/611.

2. Организациям, подведомственным или находящимся в сфере ведения Минпромторга России, выполнившим работу по категорированию объектов критической информационной инфраструктуры и имеющим значимые объекты критической информационной инфраструктуры:

2.1. Создать систему значимых объектов безопасности критической информационной инфраструктуры в соответствии с «Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утвержденными приказом ФСТЭК России от 21 декабря 2017 г. № 235 (зарегистрировано Минюстом России 22 февраля 2018 г. № 50118), при этом:

возложить на руководителя субъекта критической информационной инфраструктуры или уполномоченное им лицо функции по созданию системы безопасности, организации и контролю ее функционирования;

создать или определить структурное подразделение, ответственное за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее – структурное подразделение по безопасности), или назначить отдельных работников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее – специалисты по безопасности);

структурному подразделению по безопасности, специалистам по безопасности реализацию функций проводить во взаимодействии с подразделениями (работниками), эксплуатирующими значимые объекты критической информационной инфраструктуры, и подразделениями (работниками), обеспечивающими функционирование значимых объектов критической информационной инфраструктуры, иными подразделениями (работниками), участвующими в обеспечении безопасности значимых объектов критической информационной инфраструктуры;

применять для обеспечения безопасности значимых объектов критической информационной инфраструктуры сертифицированные на соответствие требованиям безопасности средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;

разработать и утвердить организационно-распорядительные документы по безопасности значимых объектов критической информационной инфраструктуры, определяющие порядок и правила функционирования системы

безопасности значимых объектов критической информационной инфраструктуры, а также порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры;

разработать план мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры на год;

организовать и проводить ежегодный внутренний контроль организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер.

2.2. Организовать в 2022 году и последующие годы профессиональную переподготовку, повышение квалификации работников структурных подразделений по безопасности или специалистов по безопасности по профессиональным программам в области обеспечения безопасности объектов критической информационной инфраструктуры, согласованным ФСТЭК России.

2.3. Для обеспечения устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак руководствоваться «Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239 (зарегистрировано Минюстом России 26 марта 2018 г. № 50524).

2.4. В случае изменения сведений, указанных в подпунктах «а» – «е» пункта 17 Правил категорирования объектов критической информационной инфраструктуры,[2] направлять в ФСТЭК России новые сведения в печатном и электронном виде по форме, предусмотренной пунктом 18 Правил категорирования объектов критической информационной инфраструктуры.

Срок направления: не позднее 20 рабочих дней со дня изменения сведений.

2.5. Направить сведения о результатах реализации положений Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и изданных в его исполнение нормативных правовых актов по форме № 1 (образец формы прилагается) в печатном и электронном виде на оптическом диске в:

ФГУП «НПП «ГАММА» – подведомственные Минпромторгу России организации и головные организации интегрированных структур в сфере ведения Минпромторга России;

Срок направления: до 1 июля 2022 г.

головные организации интегрированных структур – организации, входящие в состав интегрированных структур.

Срок направления: до 1 июня 2022 г.

[2] С учетом внесенных изменений, утверждённых постановлением Правительства Российской Федерации от 24 декабря 2021 г. № 2431«О внесении изменений в постановление Правительства Российской Федерации»

2.6. Подготовить и направить «Паспорт системы обеспечения безопасности значимых объектов критической информационной инфраструктуры в организации» в печатном и электронном виде (образец формы паспорта прилагается) в:

ФГУП «НПП «ГАММА» – подведомственные Минпромторгу России организации и головные организации интегрированных структур в сфере ведения Минпромторга России;

головные организации интегрированных структур – организации, входящие в состав интегрированных структур.

Сроки направления: к 1 июля 2022 г., далее ежегодно к 1 сентября (с учетом внесенных изменений).

2.7. Разработать и согласовать «План мероприятий, реализуемых организацией при установлении в отношении принадлежащих ей объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак»[3] с ФСТЭК России.

2.8. Направить в ФСТЭК России и управления ФСТЭК России по федеральным округам копию утвержденного «Плана мероприятий, реализуемых организацией при установлении в отношении принадлежащих ей объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак».[4]

2.9. Направлять информацию о выполнении пунктов 2.7 и 2.8 в:

ФГУП «НПП «ГАММА» – подведомственные Минпромторгу России организации и головные организации интегрированных структур в сфере ведения Минпромторга России;

головные организации интегрированных структур – организации, входящие в состав интегрированных структур.

[3] Разрабатывается в соответствии с «Порядком установления уровня опасности проведения целевых компьютерных атак на информационную инфраструктуру Российской Федерации», утвержденным распоряжением Секретаря Совета Безопасности Российской Федерации от 14 декабря 2020 г. № А21-68рсб

[4] В соответствии с пунктом 14 «Методического документа «Рекомендации по подготовке планов мероприятий, реализуемых субъектами критической информационной инфраструктуры Российской Федерации при установлении в отношении принадлежащим им объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак», утвержденного ФСТЭК России 9 августа 2021 г.

Форма № 1

Сведения о результатах реализации (полное наименование организации) положений Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и изданных в его исполнение нормативных правовых актов

№ п/п	Полное и сокращённое наименование организации	Адрес места расположения	Проведение работ по определению наличия в организации объектов КИИ①			Формирование и направление в центральный аппарат ФСТЭК России перечня объектов КИИ (исходящий номер и дата)③	Категорирование объектов КИИ④					Получение из центрального аппарата ФСТЭК России уведомления о включении объектов КИИ в Реестр значимых объектов КИИ РФ (исходящий номер и дата ФСТЭК России)⑥
			Номер и дата правового акта по созданию постоянно действующей комиссии②	Дата окончания выполнения работ (чч.мм.гг)	Наличие объектов КИИ (количество или отсутствуют)		Количество объектов КИИ по категориям значимости				Направление в центральный аппарат ФСТЭК России результатов категорирования объектов КИИ (исходящий номер и дата)⑤	
							1	2	3	без категории		
1	2	3	4	5	6	7	8	9	10	11	12	13
1												

Пояснения по заполнению:

1. В графе 5 указывается дата окончания работ по определению наличия объектов КИИ.
2. В графе 6 при наличии объектов КИИ **указывается их количество**, при отсутствии объектов КИИ **указывается слово "отсутствуют"**.
3. Графы 7 - 12 заполняются при определении наличия объектов КИИ, т.е. если в графе 6 указано количество объектов КИИ.

1 пункт 5 "Правил категорирования объектов критической информационной инфраструктуры Российской Федерации", утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, с учётом внесённых изменений постановлением Правительства Российской Федерации от 13 апреля 2019 г. № 452

2 пункт 11 "Правил категорирования объектов критической информационной инфраструктуры Российской Федерации", утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, с учётом внесённых изменений постановлением Правительства Российской Федерации от 13 апреля 2019 г. № 452

3 пункты 5, 15 "Правил категорирования объектов критической информационной инфраструктуры Российской Федерации", утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, с учётом внесённых изменений постановлением Правительства Российской Федерации от 13 апреля 2019 г. № 452

4 статья 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"
пункт 5 "Правил категорирования объектов критической информационной инфраструктуры Российской Федерации", утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, с учётом внесённых изменений постановлением Правительства Российской Федерации от 13 апреля 2019 г. № 452

5 пункт 5 статьи 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"
пункты 17, 18 "Правил категорирования объектов критической информационной инфраструктуры Российской Федерации", утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, с учётом внесённых изменений постановлением Правительства Российской Федерации от 13 апреля 2019 г. № 452
приказ ФСТЭК России от 22 декабря 2017 г. "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"

6 пункт 7 статьи 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Форма № 2

Сведения о структурных подразделениях и (или) отдельных работниках, ответственных за обеспечения безопасности значимых объектов КИИ*, имеющихся в (полное наименование организации)

№ п/п	Полное и сокращённое наименование организации	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов КИИ			Отдельные работники, ответственные за обеспечение безопасности значимых объектов КИИ	Сведения о специалистах								
		Полное наименование подразделения	Количество специалистов			Наименование должности с указанием подразделения	Фамилия, имя и отчество	Дата рождения	Телефон, e-mail	Дата назначения на должность	Стаж работы в области ЗИ	Образование (наименование учебного заведения, специальность по диплому, год окончания)	Переподготовка по направлению "Информационная безопасность" (наименование учебного заведения, наименование программы обучения, период обучения, кол-во часов)	Повышение квалификации (наименование учебного заведения, наименование программы обучения, период обучения, кол-во часов)
			По штату	В наличии										
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1		Отдел обеспечения безопасности значимых объектов критической информационной инфраструктуры (наименование организации)	2	1		Начальник отдела обеспечения безопасности значимых объектов критической информационной инфраструктуры (наименование организации)	Иванов Иван Иванович	11.11.1950	(1234) 12-34-56, bezop@ensk.ru	18.02.2020	2 года	Высшее. Энский государственный университет. Системотехника. 1992 год.	НОУДПО "Центр повышения квалификации специалистов по ТЗИ" (г. Воронеж) "Комплексная защита объектов информатизации" 11.07 - 26.11.2011 530 часов	ГНИИИ ПТЗИ ФСТЭК России (г. Воронеж) "Организация технической защиты конфиденциальной информации в органах государственной власти субъектов РФ" 14 - 18.01.2013 72 часа

* Создаёт или определяет руководитель субъекта КИИ в соответствии с требованиями пункта 10 «Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235 (зарегистрировано Минюстом России 22 февраля 2018 г. рег. № 50118)

Пояснения по заполнению:

1. Форма № 2 подлежит заполнению только по организациям, имеющим значимые объекты КИИ.

2. В графах 7-15 указываются сведения по всем имеющимся в наличии штатным специалистам или отдельным работникам, ответственным за обеспечение безопасности значимых объектов КИИ.

Форма № 3

Организационно-распорядительные документы по безопасности значимых объектов КИИ*

№ п/п	Полное и сокращённое наименование организации	Полное наименование документов	Утвержден		
			Наименование нормативного правового акта о введении в действие или должности лица, утвердившего документ	Номер и (или) дата	Кем и когда (дата) согласован
1	2	3	4	5	6
1		1. Документ в котором должны быт определены:			
		цели и задачи обеспечения безопасности значимых объектов КИИ;			
		основные угрозы безопасности информации и категории нарушителей;			
		основные организационные и технические мероприятия по обеспечению безопасности значимых объектов КИИ, проводимые субъектом КИИ;			
		состав и структура системы безопасности и функции её участников;			
		порядок применения, формы оценки соответствия значимых объектов КИИ и средств защиты информации требованиям по безопасности.			
		2. Модели угроз безопасности информации в отношении значимых объектов КИИ (по каждому значимому объекту КИИ в отдельности).			
		3. Документ в котором должен быть определен порядок:			
		реализации отдельных мер по обеспечению безопасности значимых объектов КИИ;			
		порядок проведения испытаний или приёмки средств защиты информации;			
		реагирования на компьютерные инциденты;			
		информирования и обучения работников;			
		взаимодействия подразделений (работников) субъекта КИИ при решении задач обеспечения безопасности значимых объектов КИИ;			
		взаимодействия субъекта КИИ с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.			
		4. Документ в котором должны быт определены:			
		правила безопасной работы работников субъекта КИИ на значимых объектах КИИ;			
		действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций.			
…					

* В соответствии с требованиями пункта 25 раздела IV «Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235 (зарегистрировано Минюстом России 22 февраля 2018 г. рег. № 50118)

Пояснения по заполнению: 1. Форма № 3 подлежит заполнению только по организациям, имеющим значимые объекты КИИ.

Форма № 4

Организационно-распорядительные документы по безопасности значимых объектов КИИ

№ п/п	Полное и сокращённое наименование организации	Полное наименование документа	Утвержден		
			Наименование нормативного правового акта о введении в действие или должности лица, утвердившего документ	Номер и (или) дата	Кем и когда (дата) согласован
1	2	3	4	5	6
1		План мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры (наименование организации) на 2021 год (или на период с 2020 по 202_ годы)*			
		Комиссия по контролю организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер в (наименование организации)			
		План контроля организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер в (наименование организации) на 202__ год			
…					

* В соответствии с требованиями пункта 29 раздела V «Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235 (зарегистрировано Минюстом России 22 февраля 2018 г. рег. № 50118)

** В соответствии с требованиями пунктов 35, 36 раздела V «Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235 (зарегистрировано Минюстом России 22 февраля 2018 г. рег. № 50118)

Пояснения по заполнению: 1. Форма № 4 подлежит заполнению только по организациям, имеющим значимые объекты КИИ.

Для служебного пользования

(по заполнении ограничительная пометка устанавливается исполнителем, но не ниже «Для служебного пользования)

Экз. № ____

ПАСПОРТ
системы обеспечения безопасности значимых объектов критической информационной инфраструктуры в
_____
(полное наименование организации)

(по состоянию на «___» _____ 20__ г.)

1. Общие сведения о субъекте критической информационной инфраструктуры

1.1 Наименование субъекта (согласно Уставу, Положению)**:**
полное:

сокращённое:

1.2 Дата государственной регистрации организации: «___» _____ 20__ г.

1.3 Основной государственный регистрационный номер (ОГРН):

1.4 Идентификационный номер налогоплательщика (ИНН):

1.5 Юридический адрес: индекс, город (область, край и т.д.), улица, дом, корпус, литера.

1.6 Адрес для открытой переписки (в т.ч. E-mail)**:**

1.7 Адрес для секретной переписки (при наличии секретного делопроизводства)**:**

1.8 Отраслевая принадлежность субъекта (наименование головной организации структуры, в состав которой входит субъект):

1.9 Сфера (область) деятельности субъекта, в которой функционирует объект критической информационной инфраструктуры:[1]

1.10 Должностные лица субъекта:
руководитель субъекта;
уполномоченное должностное лицо, на которое возложены функции обеспечения безопасности значимых объектов критической информационной инфраструктуры;
руководитель структурного подразделения, ответственного за обеспечение безопасности значимых объектов критической информационной инфраструктуры, или работники, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры.

№ п/п	Должность	Фамилия, имя и отчество	Дата рождения	С какого времени занимает должность	Номер телефона/ факсимильного аппарата, E-mail
1					
2					
3					

[1] В соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

1.11 Наличие лицензии (разрешения) ФСБ России, ФСТЭК России

№ п/п	Наименование органа ФСБ России, ФСТЭК России, выдавшего лицензию	Виды деятельности, работ	Регистрационный номер и дата лицензии	Срок действия лицензии
				до XX.XX.20XX

1.12 Постоянно действующая комиссия по категорированию объектов критической информационной инфраструктуры[2]

Номер и дата правового акта о создании комиссии:

№ п/п	Состав комиссии	Наименование должности	Фамилия, имя, отчество
1	Председатель комиссии		
2	Заместитель председателя комиссии		
3	Член комиссии		

1.12.1 Сведения о заседаниях постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры

№ п/п	Дата проведения заседания комиссии	Рассматриваемые вопросы	Принятые решения по результатам заседания комиссии	Примечание

[2] В соответствии с пунктом 11 «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации», утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, с учётом внесённых изменений постановлением Правительства Российской Федерации от 13 апреля 2019 г. № 452

1.13 Ранее проведенные проверки субъекта (ФСТЭК России или ее территориальные органы, вышестоящая организация над субъектом)

№ п/п	Наименование организации, проводившей проверку	Сроки проверки	Количество нарушений и недостатков		Фамилия, имя и отчество председателя комиссии	Выводы комиссии
			Нарушений	Недостатков		

2. Состав сил обеспечению безопасности значимых объектов КИИ[3]

2.1 Структурное подразделение (штатные специалисты) по обеспечению безопасности значимых объектов КИИ

Наименование подразделения (должности штатного специалиста)	Количество сотрудников (по штату/в наличии)	Наименование положения о структурном подразделении, должностного регламента (функциональных обязанностей) штатного специалиста, дата утверждения

2.1.1 Сведения о специалистах структурного подразделения (штатных специалистах) по обеспечению безопасности значимых объектов КИИ

№ п/п	Должность, рабочий телефон	Фамилия, имя и отчество	Дата рождения	Специальность по диплому	Стаж работы (по КИИ)	Обучение в образовательных организациях по программам, согласованным ФСТЭК России	
						Дата	Наименование учебного заведения, программы обучения, количество часов
1	2	3	4	5	6	7	8

[3] В соответствии с «Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235 (зарегистрировано Минюстом России 22 февраля 2018 г. рег. № 50118)

2.2 Сведения о подразделениях (работниках), эксплуатирующих значимые объекты КИИ

№ п/п	Наименование подразделения	Наименование должности работника	Фамилия, имя и отчество	Примечание
1	2	3	4	5

2.3 Сведения о подразделениях (работниках), обеспечивающих функционирование (сопровождение, обслуживание, ремонт) значимых объектов КИИ

№ п/п	Наименование подразделения	Наименование должности работника	Фамилия, имя и отчество	Примечание
1	2	3	4	5

2.5 Сведения об иных подразделениях (работниках), участвующих в обеспечении безопасности значимых объектов КИИ

№ п/п	Наименование подразделения	Наименование должности работника	Фамилия, имя и отчество	Примечание
1	2	3	4	5

3. Сведения о значимых объектах КИИ

№ п/п	Наименование значимого объекта КИИ	Тип объекта КИИ	Сфера/область	Категория значимости	Дата включения в Реестр значимых объектов КИИ РФ	Исходящий номер и дата уведомления ФСТЭК России о включении объектов КИИ в Реестр значимых объектов КИИ РФ	Примечание

4. Программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектах КИИ[4]

№ п/п	Сокращенное наименование значимого объекта КИИ, на котором применяются программные и программно-аппаратные средства[5]	Сведения о программных и программно-аппаратных средствах			
		Наименование	Заводской номер	Год выпуска	Реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о не проведении такой оценки[6]
1	2	3	4	5	6

[4] В соответствии с требованиями раздела III «Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235 (зарегистрировано Минюстом России 22 февраля 2018 г. рег. № 50118)

[5] В соответствии с пунктом 17 «Требований …», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235

[6] В соответствии с пунктом 18 «Требований …», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235

5. Перечень организационно-распорядительных документов по обеспечению безопасности значимых объектов КИИ[7]

№ п/п	Наименование документа	Утверждение и введение в действие	
		Наименование нормативного правового акта или должности лица, утвердившего документ	Номер и (или) дата
1	2	3	4

5. Контроль организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер[8]

5.1 Комиссия по внутреннему контролю организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер

Номер и дата правового акта о создании комиссии:

№ п/п	Состав комиссии	Наименование должности	Фамилия, имя, отчество
1	Председатель комиссии		
2	Заместитель председателя комиссии		
3	Член комиссии		

5.2 Результаты внутреннего контроля организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер

[7] В соответствии с требованиями разделов IV, V «Требований …», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235

[8] В соответствии с требованиями пунктов 35, 36 раздела V «Требований …», утверждённых приказом ФСТЭК России от 21 декабря 2017 г. № 235

№ п/п	Наименование итогового документа по результатам контроля	Должность, фамилия и инициалы лица, утвердившего документ, и дата утверждения	Наименование средств контроля (анализа) защищенности, применяемых в контроле	Нарушения и недостатки, выявленные по результатам контроля
1	Акт контроля организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер в (наименование субъекта)			

5.3 Результаты внешней оценки (внешнего аудита) состояния безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер

№ п/п	Наименование итогового документа по результатам внешней оценки (внешнего аудита)	Наименование организации, проводившей оценку (аудит), реквизиты лицензии на деятельность в области защиты информации	Наименование средств контроля (анализа) защищенности, применяемых в оценке (аудите)	Нарушения и недостатки, выявленные по результатам оценки (аудита)
1	Акт оценки (аудита) организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер в (наименование субъекта)			

6. Организационные вопросы, связанные с установлением уровня опасности проведения целевых компьютерных атак на информационную инфраструктуру[9]

6.1 Сведения о должностных лицах, ответственных за:[10]

прием информации об установлении соответствующего уровня опасности и за оперативное доведение ее до сведения руководителя субъекта;

организацию работ по выполнению плана мероприятий и взаимодействию с управлением ФСТЭК России по федеральному округу;

осуществление экстренного взаимодействия с Национальным координационным центром по компьютерным инцидентам по вопросам реагирования на компьютерные инциденты на объектах критической информационной инфраструктуры.

№ п/п	Наименование должности, фамилия, имя и отчество	Наименование, номер и дата правового акта, которым на должностных лиц возложены соответствующие обязанности	Номер абонента сети правительственной телефонной связи, рабочего, мобильного телефонов, адрес электронной почты	Исходящий номер и дата письма в управление ФСТЭК России по федеральному округу о должностных лицах, на которые возложены соответствующие обязанности
1	Ответственный за прием информации и её доведение, начальник отдела Иванов Иван Иванович			
2	Ответственный за организацию работ по выполнению плана мероприятий, главный инженер Петров Петр Петрович			
3	Ответственный за взаимодействие с НКЦКИ, начальник сектора Сидоров Алексей Николаевич			

[9] В соответствии с «Порядком установления уровня опасности проведения целевых компьютерных атак на информационную инфраструктуру Российской Федерации», утвержденным распоряжением Секретаря Совета Безопасности Российской Федерации от 14 декабря 2020 г. № А21-68рсб

[10] В соответствии с пунктом 10 «Методического документа «Рекомендации по подготовке планов мероприятий, реализуемых субъектами критической информационной инфраструктуры Российской Федерации при установлении в отношении принадлежащим им объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак», утвержденного ФСТЭК России 9 августа 2021 г.

Рекомендуется возложить обязанности за прием информации и ее доведение:

в нерабочее время на круглосуточные дежурные силы субъекта;

в рабочее время на должностных лиц (руководитель, заместитель руководителя) структурного подразделения, ответственного за обеспечение безопасности значимых объектов критической информационной инфраструктуры, или отдельных работников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры.

6.2 План мероприятий, реализуемых организацией при установлении в отношении принадлежащих ей объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак

Полное наименование плана	Согласование[11] и утверждение плана		Исходящий номер и дата сопроводительного письма копии плана в управление ФСТЭК России по федеральному округу[12]
	Наименование должности, фамилия и инициалы лица,[13] согласовавшего план, дата согласования	Наименование должности, фамилия и инициалы лица, утвердившего план, дата утверждения	

6.3 Плановые учения (тренировки) по проверке готовности к действиям при установлении соответствующего уровня опасности

Сроки проведения учения (тренировки)	Наименование должности, фамилия и инициалы руководителя учения (тренировки)	Привлекаемые силы средства	Выявленные нарушения и недостатки	Вывод о готовности организации к действиям при установлении уровня опасности

[11] В соответствии с пунктом 13 «Методического документа «Рекомендации по подготовке планов мероприятий, реализуемых субъектами критической информационной инфраструктуры Российской Федерации при установлении в отношении принадлежащим им объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак», утвержденного ФСТЭК России 9 августа 2021 г.

[12] В соответствии с пунктом 14 «Методического документа «Рекомендации …», утвержденного ФСТЭК России 9 августа 2021 г.

[13] Руководитель управления ФСТЭК России по федеральному округу или лицо его замещающее

7. Перечень филиалов, дочерних и зависимых обществ

Полное и сокращенное наименование филиалов, дочерних и зависимых обществ	Наименование должности руководителя, фамилия, имя и отчество, номер телефона	Адрес для несекретной переписки	Адрес для секретной переписки	Примечание

Руководитель организации И.Фамилия

« ___ » _____ 20 __ г.