Особенности категорирования объектов критической информационной инфраструктуры Российской Федерации в организациях здравоохранения

Гандзюк Татьяна Максимовна
Ведущий специалист-эксперт отдела
Тел.: (343) 372-18-52 (91)

Субъект КИИ в сфере здравоохранения

Субъекты КИИ - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым **на праве собственности, аренды или на ином законном основании** принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере…

Больницы, поликлиники

Медицинские лаборатории

Санатории – профилактории

Руководитель субъекта КИИ или уполномоченное им лицо

работники субъекта КИИ, являющиеся специалистами в области выполняемых функций, осуществляемых видов деятельности, в области ИТ, по эксплуатации технологического оборудования

работники структурного подразделения по ГО и ЧС или работники, уполномоченные на решение задач в этой области

Комиссия по категорированию

работники субъекта КИИ, на которых возложены функции обеспечения безопасности объектов КИИ

работники подразделения по защите государственной тайны субъекта КИИ

иные работники субъекта КИИ

В состав могут включаться представители гос. органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с ними (напр. Министерство здравоохранения)

Определение основного вида деятельности субъекта КИИ в рамках указанных сфер (областей)

Примеры основных видов деятельности:

1) деятельность по выполнению обязательств перед страховщиками по **обязательному социальному страхованию: оказание первичной медико-санитарной и специализированной медицинской помощи** в соответствии с лицензией в рамках территориальной программы обязательного медицинского страхования;

2) **высокотехнологическая медицинская помощь**, не включенная в базовую программу обязательного медицинского страхования;

3) **заготовка, хранение, транспортировка и обеспечение безопасности донорской крови** и ее компонентов;

4) **первичная медико-санитарная помощь**, не включенная в базовую программу обязательного медицинского страхования;

5) **специализированная медицинская помощь** (за исключением высокотехнологической помощи), не включенная в базовую программу обязательного медицинского страхования, по профилям;

6) обеспечение мероприятий, направленных **на охрану и укрепления здоровья**.

Определение процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ

Примеры процессов:

- **ввод и хранение данных** о проведённых манипуляциях в лечении и результатах полученных по итогу всего лечения **в электронной медицинской карте пациента**;
- **диагностические обследования** и лечебные процедуры пациентов;
- формирование **расписание приема пациентов**, в том числе резервирование времени приема для определенных категорий пациентов;
- формирование реестров и **счетов на оплату за услуги**, оказанные пациентам, застрахованным по ОМС;
- расчет **заработной платы сотрудников** учреждения;
- закупка, хранение, продажа и предоставление по рецепту **лекарственных средств**;
- планирование работы медицинских сотрудников;
- кадровый учет.

Выявление наличия критических процессов у субъекта КИИ, в рамках каждого из основных видов деятельности

Пример критических процессов:

- ввод и хранение данных о проведённых манипуляциях в лечении и результатах полученных по итогу всего лечения в электронной медицинской карте пациента;
- диагностические обследования и лечебные процедуры пациентов;
- формирование расписание приема пациентов, в том числе резервирование времени приема для определенных категорий пациентов;
- формирование реестров и счетов на оплату за услуги, оказанные пациентам, застрахованным по ОМС;
- закупка, хранение, продажа и предоставление по рецепту лекарственных средств.

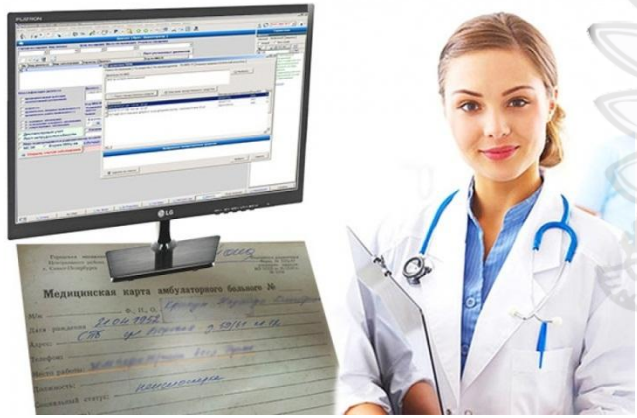
Диагностика - комплекс медицинских вмешательств, направленных на распознавание состояний или установление факта наличия либо отсутствия заболеваний, осуществляемых посредством сбора и анализа жалоб пациента, данных его анамнеза и осмотра, проведения лабораторных, инструментальных, патолого-анатомических и иных исследований в целях определения диагноза, выбора мероприятий по лечению пациента и (или) контроля за осуществлением этих мероприятий

Определение объектов КИИ

ввод и хранение данных о проведённых манипуляциях в лечении и результатах полученных по итогу всего лечения в электронной медицинской карте пациента	МИС «Промед»
диагностические обследования и лечебные процедуры пациентов	АСУ «Рентген», ИС «Анализатор»
формирование расписание приема пациентов, в том числе резервирование времени приема для определенных категорий пациентов	Нет ИС, обеспечивающей этот процесс
формирование реестров и счетов на оплату за услуги, оказанные пациентам, застрахованным по ОМС	МИС «Промед»
закупка, хранение, продажа и предоставление по рецепту лекарственных средств	ПК АСУЛОН «М-АПТЕКА»

Составление Перечня объектов КИИ

Медицинские информационные системы (ведение электронных карт пациентов, регистратура…)



АСУ хирургическим оборудованием

АСУ (ИС) диагностического оборудования (МРТ, КТ, рентген, анализатор, УЗИ…)

Информационное сообщение ФСТЭК России от 24 августа 2018 г. № 240/25/3752

Рекомендуемая форма перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

УТВЕРЖДАЮ

Должность руководителя субъекта критической информационной инфраструктуры Российской Федерации (далее – субъект) или уполномоченного им лица

Подпись руководителя субъекта или уполномоченного им лица | Фамилия, имя, отчество (при наличии) руководителя субъекта или уполномоченного им лица

«____» _____ 20____ г.

Дата утверждения перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

№ п/п	Наименование объекта	Тип объекта[1]	Сфера (область) деятельности, в которой функционирует объект [2]	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)[3]
1.					
2.					
			...		
n.					

[1] Указывается один из следующих типов объекта: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

[2] Указывается сфера (область) в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации инфраструктуры Российской Федерации».

[3] Указываются должность, фамилия, имя, отчество (при наличии) должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

Обязательное согласование только для организаций, имеющих ведомственную принадлежность (п. 15 ПП РФ № 127)

10 дней

ФСТЭК России

1 год

категорирование объектов КИИ

Обязательно: прилагать электронный вид Перечня

Типовые ошибки при составления Перечня

Представление сведений об отсутствии в организации объектов КИИ или о том, что организация не является субъектом КИИ Российской Федерации

Представление Перечней в ФСТЭК России на согласование или на утверждение

Представление в составе Перечней объектов КИИ, не принадлежащих субъекту

Не указывается контактная информация

Направление Перечня только в Управление ФСТЭК России по Уральскому федеральному округу

Не указана дата утверждения Перечня

Категорирование объектов КИИ

Акты категорирования объектов КИИ

Заполняются на основе Акта категорирования и направляются в ФСТЭК России

Остаются в организации

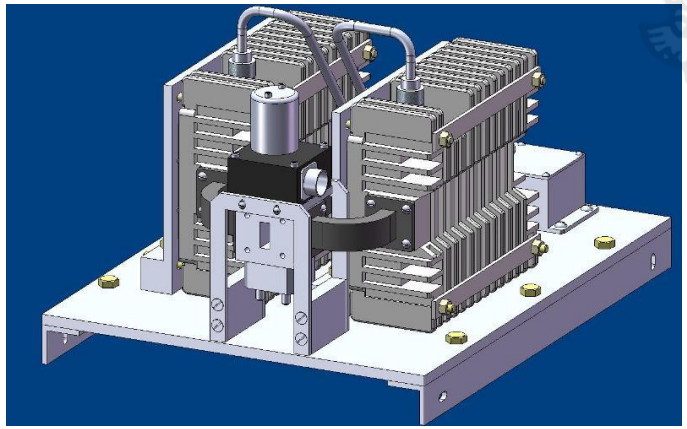
Сведения о присвоении объекту КИИ одной из категории значимости

В десятидневный срок со дня принятия субъектом КИИ соответствующего решения (о присвоении категории или отсутствии такой необходимости) направляются в ФСТЭК России

Показатели критериев значимости

Оценка производится по каждому из значений

Наличие цифровых систем резервирования, защиты и противоаварийной автоматики не учитывается

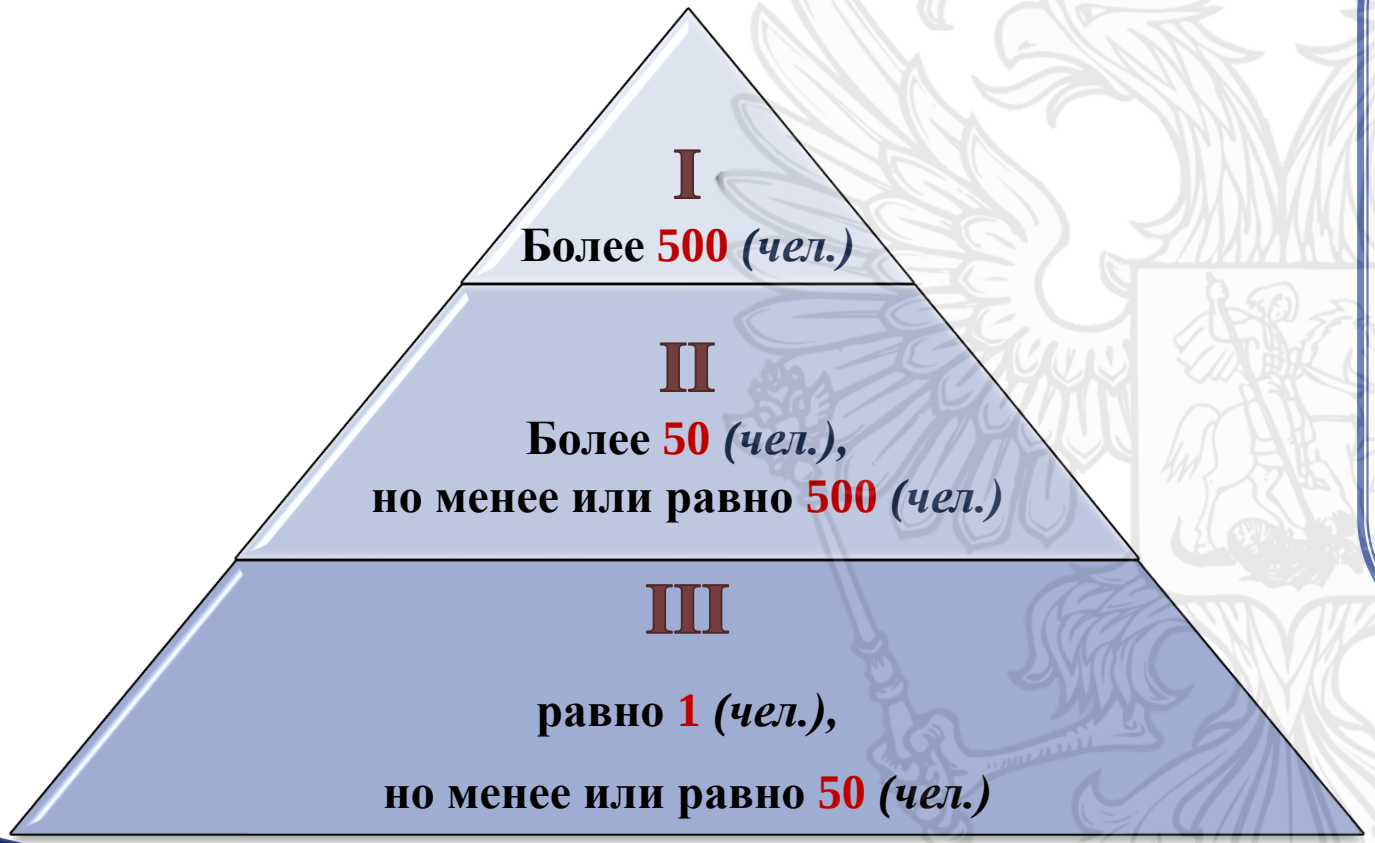


Рассматривается наихудший сценарий (целенаправленная атака) с максимально возможным ущербом

Категория присваивается по наивысшему значению

I. Социальная значимость

1.Причинение ущерба жизни и здоровью людей (человек)



- Причинение ущерба жизни людей – гибель.
- Причинение ущерба здоровью людей – нарушение анатомической целостности и физиологической функции органов и тканей человека в результате воздействия физических, химических, биологических и психических факторов внешней среды (в соответствии с правилами определения степени тяжести вреда, причиненного здоровью человека (утв. постановлением Правительства РФ от 17 августа 2007 г. № 522)

Оценивается по результатам анализа последствий возможных аварий или иных инцидентов, связанных с негативным физическим, химическим, радиационным или иным воздействием на людей, которое может быть оказано в результате нарушения функционирования объекта КИИ

5. Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)

Государственная услуга – деятельность по реализации функций соответственно федерального органа исполнительной власти, государственного внебюджетного фонда, исполнительного органа государственной власти субъекта Российской Федерации, а также органа местного самоуправления при осуществлении отдельных государственных полномочий, …, которая осуществляется по запросам заявителей в пределах установленных … полномочий органов, предоставляющих государственные услуги (в соответствии с Федеральным законом Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»)

Примеры государственных услуг

- Вызов врача на дом
- Запись на прием к врачу
- Предоставление сведений об оказанной медицинской помощи

*Реестр государственный услуг (федеральных и муниципальных) (доступ ограничен) https://frgu.gosuslugi.ru
*Портал государственных услуг Российской Федерации (доступ свободный) https://gosuslugi.ru

III. Экономическая значимость

9. Возникновение ущерба бюджетам Российской Федерации

Доходы бюджетов РФ

- Нефтегазовые
- На прибыль
- НДС
- Акцизные
- Ввозные пошлины
- Прочие

Прибыль субъекта КИИ

- 3 %* в Федеральный бюджет
- до 17 %* в региональный бюджет

*В соответствии с налоговым кодексом Российской Федерации

Типовые ошибки при заполнении Сведений о присвоении объекту КИИ одной из категории значимости

1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления, или информационно-телекоммуникационной сети)	приводится наименование субъекта, приводят сокращённое название (напр. ПК АСД ССМП АДИС)
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	не приводится почтовый индекс
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	
1.4.	Назначение объекта	приводится не полное описание
1.5.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	

Типовые ошибки при заполнении Сведений о присвоении объекту КИИ одной из категории значимости

2.1.	Наименование субъекта	
2.2.	Адрес местонахождения субъекта	
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	приводится инициалы
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта	не заполняется Прим. если нет назначенного лица, необходимо указать руководителя субъекта КИИ
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	приводится инициалы не приводятся контактные данные
2.6.	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

Типовые ошибки при заполнении Сведений о присвоении объекту КИИ одной из категории значимости

3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	приведена неверная категория сети электросвязи Прим. рекомендуем обратиться к Федеральному закону от 7 июля 2003 г. № 126-ФЗ «О связи»
3.2.	Наименование оператора связи и (или) провайдера хостинга	
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	не приведены сведения о протоколах взаимодействия
4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	приведена неверная информация (напр. ФИО сотрудника)
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	

Типовые ошибки при заполнении Сведений о присвоении объекту КИИ одной из категории значимости

4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	не приведены сведения о технологическом, производственном оборудовании (исполнительных устройствах) (напр. в АСУ «Рентген» необходимо указать сам рентген аппарат)
4.4	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	
5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	приведены прикладные программы

Типовые ошибки при заполнении Сведений о присвоении объекту КИИ одной из категории значимости

5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	приведен не полный перечень прикладного программного обеспечения
5.4.	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение)(наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	не приведены сертификаты, не полный перечень СЗИ
6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	не определена категория нарушителя, не дано его описание (кто для организации является внешним или внутренним нарушителем, его оснащённость, знания, потенциал) Прим. рекомендовано обратиться к Базовой модели угроз и БДУ

Типовые ошибки при заполнении Сведений о присвоении объекту КИИ одной из категории значимости

6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	не приведен перечень УБИ Прим. рекомендовано обратиться к Базовой модели угроз и БДУ, перечислить идентификаторы УБИ в соответствии с БДУ. Можно приложить Модель угроз
7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	не приведены типы компьютерных инцидентов либо перечень не полный
8.1.	Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категории	

Типовые ошибки при заполнении Сведений о присвоении объекту КИИ одной из категории значимости

8.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	
8.3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	
9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	не заполнено поле, не приведены реквизиты документов
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	неверное заполнение поля (Написано то же что и в пункте 5.4) Прим. рекомендовано обратиться к приказу ФСТЭК России № 239

Проверка ФСТЭК России результатов категорирования

Изменение в ППРФ № 127

Субъектам КИИ – государственным органам и государственным учреждениям утвердить до 1 сентября 2019 г. перечень объектов КИИ, подлежащих категорированию.

Рекомендовать субъектам КИИ – российским юридическим лицам и (или) индивидуальным предпринимателям утвердить до 1 сентября 2019 г. перечень объектов

В случае если объекты КИИ по одному из показателей критериев значимости отнесен к первой категории, расчет по остальным показателям критериев значимости не проводится.

По решению руководителя субъекта КИИ в состав комиссии могут быть включены работники не указанные в пункте 11 настоящих Правил подразделений, в том числе финансово-экономического подразделения.

Допускается оформление единого акта по результатам категорирования нескольких объектов КИИ, подлежащих одному субъекту КИИ

Pravo.gov.ru

Изменения в Приказ ФСТЭК России № 236

п/п	Приказ ФСТЭК России № 236	Изменения
1.1	Наименование объекта	Наименование объекта (наименование информационной системы, автоматизированной системы управления, или информационно-телекоммуникационной сети)
1.2	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта
1.5	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)

Изменения в Приказ ФСТЭК России № 236

п/п	Приказ ФСТЭК России № 236	Изменения
2.5	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)
2.6		ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта
3.2	Наименование оператора связи	Наименование оператора связи и (или) провайдера хостинга

Изменения в Приказ ФСТЭК России № 236

п/п	Приказ ФСТЭК России № 236	Изменения
3.4	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия
4.4		ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта
5.1	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество

Изменения в Приказ ФСТЭК России № 236

п/п	Приказ ФСТЭК России № 236	Изменения
5.4	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение)(наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации

Изменения в Приказ ФСТЭК России № 236

п/п	Приказ ФСТЭК России № 236	Изменения
7.2	Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2…	
8.1	Категория значимости, которая присвоена объекту	Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категории
8.2	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту
8.3		Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту

Гандзюк Татьяна Максимовна
Ведущий специалист-эксперт отдела
Тел.: (343) 372-18-52
(343) 372-18-91