Группа компаний «СКБ»

Порядок применения Федерального закона от 26.07.2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры РФ» в медицинских организациях

Технический директор ООО «СКБ» Михеев И.А.

РЕШЕНИЯ ДЛЯ БИЗНЕСА

Защищенный документооборот

Обеспечение юридически значимого, защищенного электронного документооборота, позволит автоматизировать внутренние процессы в организации, обеспечить неотказуемость действий сотрудников, защитить данные от подмены, намеренной порчи или уничтожения. Электронный документооборот позволит снизить производственные издержки при использовании электронной подписи для согласования и подписания документов.

Сравнение документов

Сравнение двух версий документа в различных форматах. Позволяет быстро выявлять значимые несоответствия в тексте и помогает предотвратить подписание или публикацию некорректной версии документа или договора, выявлять актуальные версии документов.

Средства организации совместной работы

Повысьте эффективность своих сотрудников внедрив системы организации совместной работы. Данные системы позволяют организовать централизованное хранилище данных, CRM системы, строить системы отчетности для наглядного анализа выполненных работ и достигнутых результатов. Данные системы могут быть как "облачными", так и располагаться на вычислительных ресурсах организации.

КОНТАКТЫ

Техническая защита информации
8 (3812) 532018
tech@ooo-skb.ru

Криптографическая защита информации
8 (3812) 377550
pki@ooo-skb.ru

ООО «СКБ»
г.Омск, ул.Ленина, д.20, оф.422
info@ooo-skb.ru

Московский филиал ООО «СКБ»
г. Москва, пр-т Волгоградский, дом 96 к.1

Белгородский филиал ООО «СКБ»
г.Белгород, ул. 5 Августа, д.135
skb31@ooo-skb.ru

ООО «СКБ-сервис»
г.Омск, ул.Ленина, д.20, оф.423
service@ooo-skb.ru

ГРУППА КОМПАНИЙ
СКБ

Кто владеет информацией,
тот владеет миром.
Натан Майер фон Ротшильд

10 ЛЕТ НА РЫНКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

www.ooo-skb.ru

О КОМПАНИИ

Группа компаний «СКБ»- системный интегратор в области обеспечения безопасности информации. Поставщик технических средств и систем защиты информации, законченных решений в виде защищенных систем обработки и сетей передачи данных.

Услуги, предоставляемые группой компаний:

- Аудит безопасности информационных систем
- Проектирование, создание, аттестация и техническая поддержка систем защиты информации
- Построение защищенных сетей передачи данных (VPN)
- систем защиты виртуальной инфраструктуры.
- Поставка, установка, настройка, сервисное обслуживание средств защиты информации
- Подбор и внедрения решений по контролю внутренних информационных потоков с защитой конфиденциальной информации от утечки.
- Защита информации при использовании облачных технологий, мобильных устройств
- Аутсорсинг систем обеспечения безопасности информационно телекоммуникационных систем
- Обеспечение юридической значимости документооборота
- Предоставление услуг аккредитованного Удостоверяющего центра

Деятельность осуществляется на основании лицензий

Управления Федеральной службы безопасности Российской Федерации по Омской области

Федеральной службы по техническому и экспортному контролю

РЕШЕНИЯ ДЛЯ БИЗНЕСА

Контроль эффективности персонала

Системы позволяющие проводить анализ эффективности работы и учет рабочего времени сотрудника, предотвращать нецелевое использование ресурсов предприятия (печать личных документов, использование соц. сетей, поиск работы…).

Защита от утечек коммерческой тайны

Использование систем защиты от утечек конфиденциальной информации (DLP) позволит Вам предотвратить вывод ценной информации на флешки, отправку по электронной почте, загрузку в облачные хранилища или разглашение коммерческой таны в переписки в популярных мессенджерах и соц. сетях (ICQ, Mail.RU, Jabber, WhatsApp и т.д.). Наличие встроенных шаблонов и возможность тонкой настройки под Ваши нужды позволит свести к минимуму утечку баз данных клиентов, финансовую документацию, интеллектуальную собственность и другую, критичную для Вашего бизнеса информацию.

Защита информации на мобильных устройствах

Данные решения позволяют обеспечить защиту важной информации хранящейся и обрабатываемой на мобильных устройствах сотрудников. Возможна организация защищенного канала связи с офисами для получения постоянного и защищенного доступа к данным хранящимся на локальных серверах организации. Для обеспечения безопасной работы сотрудников возможно проводить централизованную установку приложений и политик безопасности.

Защита данных на рабочих станциях, серверах и управление рабочими станциями

Для обеспечения защиты информации, в т.ч. коммерческой тайны, ГК "СКБ" предлагает реализовать следующий комплекс мероприятий:

- Шифрование файлов на рабочих станциях и серверах;
- Резервное копирование информации для обеспечения гарантированного восстановления данных и защиты от удаления, вирусов, изменения важных данных;
- Средства удаленного управления рабочими станциями, позволяющие производить настройку рабочих станций с одного рабочего места;
- Выявление и устранение угроз для рабочих станций и серверов;
- Контроль посещений сайтов, сотрудниками организации (социальные сети, поиск работы, сайты знакомств и т.д.);
- Защита рабочих станций от несанкционированного доступа;
- Системы обнаружения таргетированных атак;
- Антивирусная защита предприятия;
- Обслуживание систем защиты информации и аутсорсинг информационной безопасности;

Результаты работы по вопросам КИИ в области здравоохранения за 2018 год

- Оказаны услуги по вопросам категорирования объектов критической информационной инфраструктуры более чем в 80 медицинских учреждениях Омской области.
- Проанализированы характеристики, среды функционирования, угрозы информационной безопасности более чем 800 информационных систем, медицинских комплексов и отдельных медицинских устройств.
- **Получены положительные решения о внесении выделенных нами значимых объектов КИИ в Реестр значимых объектов КИИ ФСТЭК России.**

Система нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры

Федеральный закон от 26 июля 2017 г. № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

Нормативные правовые акты Президента Российской Федерации

- Указ Президента РФ от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085»
- Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
- Указ Президента РФ от 2 марта 2018 г. № 98 «О внесении изменений в Перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30 ноября 1995 г. № 1203»

Нормативные правовые акты Правительства Российской Федерации

- Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»
- Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры»
- Проект постановления Правительства РФ «Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ»

Нормативные правовые акты федеральных органов исполнительной власти

- Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов КИИ» (зарегистрирован Минюстом России 22 февраля 2018 г., рег. № 50118)
- Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости» (зарегистрирован Минюстом России 13 апреля 2018 г., рег. № 50753)
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ» (зарегистрирован Минюстом России 26 марта 2018 г., рег. № 50524)
- Приказ ФСТЭК России от 11 декабря 2017 г. № 229 «Об утверждении формы акта проверки» (зарегистрирован Минюстом России 28 декабря 2017 г., рег. № 49500)
- Приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении порядка ведения реестра значимых объектов КИИ» (зарегистрирован Минюстом России 8 февраля 2018 г., рег. № 49966)

- Приказ ФСБ России «Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам»
- Приказ ФСБ России «Об утверждении перечня информации, представляемой в ГосСОПКА и порядка ее представления»
- Приказ ФСБ России «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах и реагирования на них»
- Приказ ФСБ России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак»
- Приказ ФСБ России «Об утверждении порядка об обмене информации о компьютерных инцидентах между субъектами КИИ»
- Приказ Минкомсвязи России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак на сетях связи»
- Приказ ФСБ России «Об утверждении требований к средствам обнаружения, предупреждения и ликвидации компьютерных атак»

Разработка нормативных правовых актов по обеспечению безопасности критической информационной инфраструктуры

Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21

Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31

Устойчивое функционирование критической информационной инфраструктуры РФ при проведении в отношении ее компьютерных атак

Цель реализации Федерального закона «О безопасности критической информационной инфраструктуры РФ»

Термины и определения

Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Критическая информационная инфраструктура (КИИ) - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов

п. 6 ст. 2 Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Под сетями электросвязи следует понимать технологические системы, обеспечивающие один или несколько видов передач:
телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений,
включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- или проводного вещания.

п. 2, 24, 28 и 35 ст. 2 Федерального закона Федерального закона от 07.07.2003 N 126-ФЗ «О связи»

Объекты КИИ - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры

п. 7 ст. 2 Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Объекты КИИ - (информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления) **функционирующие в сфере здравоохранения, и принадлежащие** на праве собственности, аренды или на ином законном основании **государственным органам, государственным учреждениям, российским юридическим лицам и (или) индивидуальным предпринимателям.**

Сводное определение

Группа компаний «СКБ»

Субъекты критической информационной инфраструктуры - **государственные органы**, **государственные учреждения**, российские юридические лица и (или) индивидуальные предприниматели, **которым на праве собственности, аренды или на ином законном основании** (прокат, дарение, совместное пользование и т.п.) **принадлежат объекты КИИ, функционирующие в сфере здравоохранения**, **российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.**

п. 8 ст. 2 Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации

п. 4 ст. 2 Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Безопасность критической информационной инфраструктуры - **состояние защищенности** критической информационной инфраструктуры, **обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак**

п. 2 ст. 2 Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Этап I.
Организационно-распорядительный

Задачи этапа:

1. Сформировать структуру управления процессом обеспечения безопасности КИИ медицинской организации.
2. Сформировать и утвердить перечень (план) мероприятий по обеспечения безопасности КИИ медицинской организации.

Мероприятия:

1. Назначение, из состава руководящих работников медицинской организации, лица, уполномоченного по вопросам организации обеспечения безопасности объектов КИИ.
2. Создание структурного подразделения и (или) назначение работников организации, на которых возложены функции обеспечения безопасности объектов КИИ.
3. Создание постоянно действующей комиссии по категорированию объектов КИИ медицинской организации.

При принятии решения о создании структурного подразделения и (или) назначении работников организации, на которых возложены функции обеспечения безопасности объектов КИИ нужно учитывать требования Приказа ФСТЭК России от 21.12.2017 № 235:

- Работники структурного подразделения по безопасности, специалисты по безопасности должны обладать знаниями и навыками, необходимыми для обеспечения безопасности объектов КИИ.
- Не допускается возложение на структурное подразделение по безопасности, специалистов по безопасности функций, не связанных с обеспечением безопасности объектов КИИ или обеспечением информационной безопасности субъекта КИИ в целом.
- Для выполнения функций структурного подразделения по безопасности, субъектами КИИ могут привлекаться организации, имеющие в зависимости от информации, обрабатываемой значимым объектом КИИ, лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации (далее - лицензии в области защиты информации).

Этап II.
Категорирование объектов КИИ

Статья 7 Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Категорирование объекта КИИ - **установление соответствия** объекта КИИ **критериям значимости и показателям их значений, присвоение** ему **одной из категорий значимости, проверка сведений о результатах ее присвоения**

п. 1 ст. 7 Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

В каком порядке?

ПОСТАНОВЛЕНИЕ
от 8 февраля 2018 г. № 127

ОБ УТВЕРЖДЕНИИ ПРАВИЛ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, А ТАКЖЕ ПЕРЕЧНЯ ПОКАЗАТЕЛЕЙ КРИТЕРИЕВ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И ИХ ЗНАЧЕНИЙ

Что подлежит категорированию?

Категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры.

Кто категорирует?

Приказом по организации создается комиссия по категорированию объектов КИИ

Кто входит в комиссию?

1. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо (должностное лицо не ниже заместителя руководителя)

Кто входит в комиссию?

2. Работники субъекта КИИ, являющиеся специалистами в области осуществляемых видов деятельности, и в области информационных технологий и связи, а также специалисты по эксплуатации основного технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов.

Кто входит в комиссию?

3. Работники субъекта критической информационной инфраструктуры, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов критической информационной инфраструктуры.

Кто входит в комиссию?

4. Работники подразделения по защите государственной тайны субъекта критической информационной инфраструктуры (в случае, ***если объект КИИ обрабатывает информацию, составляющую государственную тайну***).

Кто входит в комиссию?

5. Работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций.

Кто главный?

Комиссию по категорированию возглавляет **руководитель** субъекта критической информационной инфраструктуры **или уполномоченное им лицо**

Что нужно сделать?

1. Определить управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности

Неужели все процессы в организации? Ведь их очень много!

Да, но работу можно оптимизировать, рассмотрев только те процессы, при осуществлении которых используются объекты КИИ.

А на простом языке?

Процессы, при осуществлении которых используются компьютеры, компьютеризированное оборудование, компьютерные программы, базы данных и (или) сети связи (*в том числе вычислительные сети*).

А есть шпаргалка?

Методические рекомендации по обеспечению функциональных возможностей медицинских информационных систем медицинских организаций, Минздрав России 1 февраля 2016 года.

(1 модуль МИС = 1 технологическому процессу)

А есть шпаргалка?

Методические рекомендации по обеспечению функциональных возможностей региональных медицинских информационных систем (РМИС), Минздрав России 23 июня 2016 года.

(1 модуль РМИС = 1 технологическому процессу)

А есть шпаргалка?

http://www.idmz.ru/jurnali/vrach-i-informatsionnye-tekhnologii

Какие из выделенных процессов нужно учитывать при категорировании?

Нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее - критические процессы)

Как определить перечень негативных последствий?

Виды негативных последствий перечислены в Перечне показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (Утвержден постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127)

Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (Утвержден постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127)

Утвержден
постановлением Правительства
Российской Федерации
от 8 февраля 2018 г. N 127

ПЕРЕЧЕНЬ
ПОКАЗАТЕЛЕЙ КРИТЕРИЕВ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И ИХ ЗНАЧЕНИЯ

Показатель	Значение показателя		
	III категория	II категория	I категория
I. Социальная значимость			
1. Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500

Какие типовые негативные последствия характерны для процессов в медицинской организации?

Социальные:

1. Причинение ущерба жизни и здоровью людей (от 1 человека).
2. Отсутствие доступа к государственной услуге (Перечень услуг в сфере здравоохранения, возможность предоставления которых гражданам в электронной форме посредством единого портала государственных и муниципальных услуг обеспечивает единая государственная информационная система в сфере здравоохранения, утверждён распоряжением Правительства Российской Федерации от 15 ноября 2017 г. № 2521-р).

Какие типовые негативные последствия характерны для процессов в медицинской организации?

Политические (для бюджетных учреждений):

1.Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия).

Например: БУЗОО являются некомерческими организациями, созданными Омской областью для выполнения работ, оказания услуг, в целях обеспечения реализации предусмотренных законодательством РФ полномочий Министерства здравоохранения Омской области.

Какие типовые негативные последствия характерны для процессов в медицинской организации?

Экономические (для бюджетных учреждений):

1.Возникновение ущерба субъекту КИИ, который является ***государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства***, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности).

Как оформить перечень процессов?

ПЕРЕЧЕНЬ
критических процессов в рамках осуществления деятельности медицинской организации

№ п/п	Наименование процесса	Типы инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак	Возможные негативные последствия при нарушении и (или) прекращении**		
			социальные	политические	экономические
1.	Запись пациентов на приемы врача с помощью электронных талонов (в том числе интеграция с региональным порталом записи к врачу через Интернет, федеральным сервисом записи к врачу через Интернет (ФЭР)).	Отсутствие доступа к государственной услуге, невозможность своевременного оказания медицинской (в том числе лицам с ограниченной подвижностью)	Причинение ущерба жизни и здоровью людей (человека)	Отсутствие доступа к государственной услуге, Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Возникновение финансового ущерба субъекту критической информационной инфраструктуры, организацией с участием государства в виде недополучения прибыли (невыполнение плана приема пациентов, не оказание платных услуг)

Критические процессы определили, что дальше?

Выявляются объекты критической информационной инфраструктуры (ИС, ИТКС и АСУ), которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов

Какие типовые объекты КИИ характерны для медицинской организации?

1.Медицинская информационная система.
2.Лабораторная информационная система.
3.Радиологические информационные системы (МРТ, МСКТ, рентген-аппараты, маммографы, и т.п.).
4.Автоматизированные системы управления лабораторным или диагностическим оборудованием, оборудованием по производству лекарственных средств.
5.Технологическая сеть (передачи данных) учреждения.
6.Автоматизированная система доступа к ведомственной/региональной сети системы здравоохранения.

Какие объекты КИИ можно исключить из рассмотрения?

Полностью автономные устройства ***(функционирующие без подключения к ЭВМ и сетям передачи данных)***.

Объекты КИИ выявили, что дальше?

Оформляется проект перечня объектов критической информационной инфраструктуры, подлежащих категорированию.

Форма перечня объектов критической информационной инфраструктуры, подлежащих категорированию

Приложение 1
к информационному сообщению
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.					

Проект перечня объектов критической информационной инфраструктуры, подлежащих категорированию

Направляется (*без подписи руководителя МО!*) отраслевому регулятору для согласования (например, Минздрав Омской области) для согласования.

Согласованный отраслевым регулятором перечень объектов критической информационной инфраструктуры, подлежащих категорированию

Направляется (*в течении 5 дней с момента утверждения руководителем МО*) в Центральный аппарат ФСТЭК России.

Перечень направили, что дальше?

1. Рассматриваются возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации. (Модель нарушителя)
2. Рассматриваются возможные угрозы безопасности информации.(Модель угроз)

Модель нарушителя и угроз безопасности оформляются на каждый объект КИИ?

Модель угроз безопасности информации может разрабатываться для нескольких значимых объектов, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности информации.

(Часть 11.1 Приказа ФСТЭК России от 25.12.2017 № 239)

По какой методике формируются модель нарушителя и модель угроз?

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ (ФСТЭК России)
о методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации
от 4 мая 2018 г. № 240/22/2339

Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г., а также Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г., могут применяться для моделирования угроз безопасности информации на значимых объектах критической информационной инфраструктуры Российской Федерации до утверждения ФСТЭК России соответствующих методических документов.

По какой методике формируются модель нарушителя и модель угроз?

При моделировании угроз информационной безопасности обязательно применение Банка данных угроз безопасности информации, созданного ФСТЭК России.

Банк данных доступен по адресу: https://bdu.fstec.ru/

Модель нарушителя и угроз безопасности составлены, что дальше?

Анализируются риски (уровень негативных последствий) от реализации угроз безопасности информации и сравниваются с:

Утвержден
постановлением Правительства
Российской Федерации
от 8 февраля 2018 г. N 127

ПЕРЕЧЕНЬ
ПОКАЗАТЕЛЕЙ КРИТЕРИЕВ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И ИХ ЗНАЧЕНИЯ

Показатель	Значение показателя		
	III категория	II категория	I категория
I. Социальная значимость			
1. Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500

Оценили, что делать дальше?

Оформляется акт категорирования, который должен содержать сведения об объекте КИИ, результаты анализа угроз безопасности информации объекта КИИ, реализованные меры по обеспечению безопасности КИИ, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, установленными ФСТЭК России

Акт с результатами категорирования

- подписывается членами комиссии по категорированию и утверждается руководителем субъекта критической информационной инфраструктуры;
- хранится субъектом КИИ до вывода из эксплуатации объекта критической информационной инфраструктуры или до изменения категории значимости.

Завершение категорирования

Субъект КИИ в течение 10 дней со дня утверждения акта категорирования направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

(*состав сведений утвержден частью 17 Постановления Правительства РФ от 08.02.2018 № 127,*

форма утверждена Приказом ФСТЭК России от 22.12.2017 № 236)

Можно выдохнуть, пока ожидаем решения ФСТЭК России о правильности нашего категорирования

На рассмотрение ФСТЭК России сведений о категорировании отводится 30 дней, плюс 10 дней на направления субъекту КИИ решения.

Что если ФСТЭК России **не согласиться** с результатами категорирования?

ФСТЭК России **в десятидневный срок со дня поступления представленных сведений возвращает их** в письменном виде субъекту КИИ **с мотивированным обоснованием причин возврата.**

Субъект КИИ **после получения мотивированного обоснования причин возврата** сведений о категорировании объектов КИИ, **не более чем в десятидневный срок устраняет отмеченные недостатки и повторно направляет такие сведения.**

Что если ФСТЭК России **согласиться** с результатами категорирования?

ФСТЭК России вносит сведения о таком объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры, о чем в десятидневный срок уведомляется субъект критической информационной инфраструктуры.

Этап III. Создание и эксплуатация системы безопасности значимых объектов КИИ

Руководящие документы

Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, Утверждены приказом ФСТЭК России от 21 декабря 2017 г. N 235

Руководящие документы

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, Утверждены приказом ФСТЭК России от 25 декабря 2017 г. N 239

Основные требования

Руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо, на которое возложены функции обеспечения безопасности значимых объектов критической информационной инфраструктуры (далее - уполномоченное лицо), ***создает систему безопасности, организует и контролирует ее функционирование***.

Основные требования

Руководитель субъекта критической информационной инфраструктуры ***определяет состав и структуру системы безопасности, а также функции ее участников*** при обеспечении безопасности значимых объектов критической информационной инфраструктуры в зависимости от количества значимых объектов критической информационной инфраструктуры, а также особенностей деятельности субъекта критической информационной инфраструктуры

Основные требования

Руководитель субъекта критической информационной инфраструктуры ***создает или определяет структурное подразделение***, ответственное за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее - структурное подразделение по безопасности), ***или назначает отдельных работников***, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее - специалисты по безопасности).

Основные требования

Структурное подразделение по безопасности, специалисты по безопасности ***реализуют функции*** по обеспечению безопасности значимых объектов КИИ ***во взаимодействии с подразделениями (работниками), эксплуатирующими значимые объекты*** критической информационной инфраструктуры, ***и подразделениями (работниками), обеспечивающими функционирование значимых объектов*** критической информационной инфраструктуры.

Основные требования

Подразделения, эксплуатирующие значимые объекты критической информационной инфраструктуры, ***должны обеспечивать безопасность эксплуатируемых ими значимых объектов*** критической информационной инфраструктуры. ***Объем возлагаемых на подразделения задач определяется*** субъектом критической информационной инфраструктуры ***в организационно-распорядительных документах*** по безопасности значимых объектов.

Основные требования

Сертифицированные средства защиты информации применяются в случаях, установленных законодательством Российской Федерации (например: когда значимый объект КИИ является ИСПДн/ГИС), а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической КИИ самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации

Основные требования

Субъектом критической информационной инфраструктуры в рамках функционирования системы безопасности должны быть утверждены организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила функционирования системы безопасности значимых объектов, а также порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Основные требования

При построении системы безопасности (далее – СБ)отдельных значимых объектов должны быть:

1. Разработано техническое задание на создание СБ.
2. Разработан технический проект и эксплуатационная документация на СБ в целом, и её компоненты.
3. Приобретены, установлены и настроены средства защиты.
4. Внедрены организационные меры обеспечения безопасности.
5. Проведены эксплуатационные и приемочные испытания СБ

Основные требования

В рамках функционирования системы безопасности субъектом критической информационной инфраструктуры должны быть внедрены следующие процессы:

- планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;
- реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;
- контроль состояния безопасности значимых объектов критической информационной инфраструктуры;
- совершенствование безопасности значимых объектов критической информационной инфраструктуры.

Основные требования

Контроль эффективности системы безопасности проводится ежегодно комиссией, назначаемой субъектом критической информационной инфраструктуры. В состав комиссии включаются работники структурного подразделения по безопасности, специалисты по безопасности, работники подразделений, эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений, обеспечивающих функционирование значимых объектов критической информационной инфраструктуры.

Основные требования

В случае проведения по решению руководителя субъекта критической информационной инфраструктуры **внешней оценки (внешнего аудита)** состояния безопасности значимых объектов критической информационной инфраструктуры **внутренний контроль может не проводиться**.

Спасибо за внимание!

Технический директор ООО «СКБ» Михеев И.А.,

тел. (3812) 53-20-18, e-mail: imiheev@ooo-skb.ru