Типовой план мероприятий

по реализации Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и принятых в соответствии с ним нормативных правовых актов

№	Мероприятие	Ответственный	Срок
1	Создать комиссию по категорированию объектов критической информационной инфраструктуры (далее – КИИ)	субъект КИИ	до 30.06.2018
2	Разработать перечень объектов КИИ, подлежащих категорированию, и направить их в ФСТЭК России	субъект КИИ	до 01.08.2018
3	Провести категорирование объектов КИИ в соответствии с утвержденным перечнем и направить результаты категорирования в ФСТЭК России	субъект КИИ	до 30.11.2018
4	Создать (уточнить созданные) систем безопасности, включающих в том числе назначение руководящего должностного лица, ответственного за организацию и контроль обеспечения безопасности значимых объектов критической информационной инфраструктуры, создание (назначение) структурного подразделения, ответственного за обеспечение безопасности значимых объектов критической информационной инфраструктуры, а также разработку организационно-распорядительных документов по вопросам обеспечения безопасности критической информационной инфраструктуры	субъект КИИ	до 01.12.2018
5	Провести анализ и при необходимости привести отраслевые (ведомственные) или локальные акты, регламентирующие вопросы обеспечения информационной безопасности и защиты информации, в соответствие с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации».	субъект КИИ	до 31.12.2018
6	Спланировать и провести с работниками, выполняющими функции	субъект КИИ	до 15.02.2019

	с использованием значимых объектов критической информационной инфраструктуры, учебные занятия, в ходе которых проинформировать их о действующих требованиях по обеспечению безопасности значимых объектов критической информационной инфраструктуры и наиболее актуальных угрозах безопасности информации.		
7	При создании (модернизации) значимых объектов критической информационной инфраструктуры включать в технические задания на требования по обеспечению их безопасности, установленные пунктом 10 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 239.	субъект КИИ	постоянно
8	Обеспечить реализацию первоочередных мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры в соответствии с пунктом 22 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 239	субъект КИИ	до 31.12.2018

Первоочередные меры
по обеспечению безопасности значимых объектов критической информационной инфраструктуры

В соответствии с пунктом 22 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 239, к первоочередным мерам по обеспечению безопасности значимых объектов критической информационной инфраструктуры относятся:

1. выявление инцидентов безопасности в автоматизированных (информационных) системах и реагирование на них;

2. управление конфигурацией автоматизированной (информационной) системы; своевременное обновление программного обеспечения с целью устранения уязвимостей в нем;

3. исключение использования слабых паролей (паролей менее 6 буквенно-цифровых символов, словарных паролей типа «admin», «qwerty 123», «P@swOrd» и им аналогичных);

4. исключение при доступе в автоматизированные (информационные) системы и к их компонентам использование аутентификационной информации (паролей, пин-кодов), заданной по умолчанию производителями программного обеспечения и (или), используемой при настройках системы (средств) защиты информации информационной системы на этапах проектирования;

5. исключение хранения конфигурационных файлов сетевого оборудования, идентификационной и аутентификационной информации и других критичных системных данных в открытом виде на узлах информационной системы;

6. обеспечение разделения функций в автоматизированной (информационной) системе по администрированию (системного администратора) и администрированию средств защиты информации (администратора безопасности), предусмотрев заведение отдельных учетных записей и разных полномочий для указанных категорий привилегированных пользователей;

7. обеспечение сегментирования автоматизированной (информационной системы), как минимум, выделение в отдельный сегмент рабочих мест для управления (администрирования);

8. регламентацию порядка подключения и доступа к ресурсам информационной системы мобильных устройств пользователей, исключения несанкционированных подключений мобильных устройств и беспроводных точек доступа;

9. периодический контроль за обеспечением уровня защищенности автоматизированных (информационных) систем.