# **Приказ Федеральной службы безопасности Российской Федерации от 19.06.2019 № 281 "Об утверждении Порядка, технических условий установки** **и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак** **и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак** **в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации****"**

В соответствии с пунктом 10 части 4 статьи б Федерального закона от 26 июля 2017 г. № 187-ФЗ «O безопасности критической информационной инфраструктуры Российской Федерации»

**П Р И К А З Ы В А Ю**

утвердить прилагаемые Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования
на компьютерные инциденты, за исключением средств, предназначенных
для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации.

Директор

А.Бортников

Приложение

к приказу ФСБ РФ

от 19 июня 2019 г. N 281

### **Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признако**

1. Настоящие Порядок и технические условия регулируют установку
и эксплуатацию средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования
на компьютерные инциденты, за исключением средств, предназначенных
для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации (далее – средства, критическая информационная инфраструктура соответственно), в том числе в банковской сфере и в иных сферах финансового рынка.

2. Для согласования установки средств субъект критической информационной инфраструктуры не позднее чем за 45 календарных дней
до даты планируемой установки направляет в ФСБ России структурно-функциональную схему подключения средств к информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, а также сведения:
об устанавливаемых средствах (наименование, предназначение,
версия (при наличии);
о местах установки средств (место нахождения
или географическое местоположение зданий или сооружений, в которых планируется установка средств);
о лицах, ответственных за эксплуатацию средств (фамилия, имя, отчество (при наличии), должность, телефонные номера);
о контролируемых средствами объектах критической информационной инфраструктуры (наименования информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления).

3. ФСБ России в срок до 45 календарных дней с даты поступления рассматривает представленные сведения на предмет отсутствия или наличия оснований для отказа в согласовании установки средств.
По результатам рассмотрения представленных сведений ФСБ России подготавливает и направляет субъекту критической информационной инфраструктуры письмо о согласовании или об отказе в согласовании установки средств.

4. Субъект критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, должен направить информацию, указанную в пункте 2 настоящих Порядка и технических условий, в Банк России в течение 5 календарных дней с даты получения письма ФСБ России о согласовании.

5. Изменение структурно-функциональной схемы подключения средств к информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, состава установленных средств и (или) мест их установки осуществляется субъектом критической информационной инфраструктуры по согласованию с ФСБ России в порядке, предусмотренном пунктом 2 настоящих Порядка и технических условий.
При изменении иной информации, указанной в пункте 2 настоящих Порядка и технических условий, субъект критической информационной инфраструктуры информирует ФСБ России в течение 5 календарных дней
со дня ее изменения.
При изменении информации, указанной в пункте 2 настоящих Порядка и технических условий, субъект критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере
и в иных сферах финансового рынка, информирует Банк России в течение 5 календарных дней со дня ее изменения.

6. Установка, настройка, проверка работоспособности
и подключение средств к информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления проводятся субъектом критической информационной инфраструктуры
и (или) привлекаемой в соответствии с законодательством
Российской Федерации субъектом критической информационной инфраструктуры организацией, осуществляющей лицензируемую деятельность в области защиты информации, и осуществляются
в соответствии с эксплуатационной документацией на данные средства.
При этом установка средств не должна нарушать функционирование информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления объекта критической информационной инфраструктуры.

7. Субъект критической информационной инфраструктуры после приема в эксплуатацию средств информирует об этом Национальный координационный центр по компьютерным инцидентам
в течение 5 календарных дней.

8. В целях непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации субъект критической информационной инфраструктуры обеспечивает круглосуточную
и бесперебойную работу средств.

9. Субъект критической информационной инфраструктуры определяет порядок доступа к эксплуатируемым средствам и осуществления контроля
за ним.

10. Эксплуатация и техническое обслуживание средств осуществляется субъектом критической информационной инфраструктуры
и (или) привлекаемой в соответствии с законодательством
Российской Федерации субъектом критической информационной инфраструктуры организацией, осуществляющей лицензируемую деятельность в области защиты информации, в соответствии
с эксплуатационной документацией на данные средства.

11. При аварийном отключении электропитания субъект критической информационной инфраструктуры должен обеспечивать работу средств
в текущем режиме или правильное (корректное) завершение их работы
с реализацией функции автоматического оповещения лиц, ответственных
за эксплуатацию средств.