

Приложение
к приказу ФСБ России
от
№

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

1. Настоящие порядок и технические условия регламентируют порядок и 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 (далее – средства и КИИ соответственно), в том числе в банковской сфере и в иных сферах финансового рынка.

2. Субъект КИИ согласовывает с Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ) установку средств.

3. Для согласования установки средств субъект КИИ направляет в НКЦКИ в определяемом им формате следующие сведения:

- о средствах (наименование, предназначение, производитель, версия (при наличии));

- о лицах, ответственных за эксплуатацию средств (фамилия, имя, отчество (при наличии), должность, контактный телефон);

- о контролируемых средствами объектах КИИ (наименование информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем);

о местах установки средств (почтовые адреса зданий, в которых планируется установка средств).

Согласование производится в срок до 45 календарных дней.

4. Субъект КИИ информирует НКЦКИ об изменении сведений, указанных в пункте 3 настоящих порядка и технических условий, в течение 5 календарных дней со дня их изменения.

5. Место установки средств определяется субъектом КИИ самостоятельно.

6. Установка, настройка, проверка работоспособности и подключение средств к информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам проводятся субъектом КИИ и (или) в соответствии с заключаемыми субъектом КИИ договорами организацией, осуществляющей на основании лицензии деятельность в области защиты информации, не являющейся субъектом КИИ (далее – организация, осуществляющая деятельность в области защиты информации), и осуществляются в соответствии с эксплуатационной документацией на средства.

7. Прием в эксплуатацию установленных средств осуществляется субъектом КИИ самостоятельно.

8. Субъект КИИ после приема в эксплуатацию средств информирует об этом НКЦКИ.

9. Субъектом КИИ должна быть обеспечена круглосуточная и бесперебойная работа средств. При этом субъектом КИИ определяется порядок доступа к эксплуатируемым средствам и осуществления контроля за ним.

10. Эксплуатация и техническое обслуживание средств осуществляются субъектом КИИ и (или) организацией, осуществляющей деятельность в области защиты информации, в соответствии с эксплуатационной документацией на средства.

11. При аварийном отключении электропитания субъектом КИИ должно обеспечиваться продолжение работы средств в текущем режиме или корректное автоматическое завершение их работы с оповещением субъекта КИИ.

12. Восстановление работоспособности средств после сбоя или отказа должно осуществляться в максимально короткие сроки, в том числе с использованием запасных инструментов и принадлежностей средств.