МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от ___ декабря 2017 г. № ____

ОБ УТВЕРЖДЕНИИ ПОРЯДКА, ТЕХНИЧЕСКИХ УСЛОВИЙ УСТАНОВКИ И ЭКСПЛУАТАЦИИ СРЕДСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ПОИСКА ПРИЗНАКОВ КОМПЬЮТЕРНЫХ АТАК В СЕТЯХ ЭЛЕКТРОСВЯЗИ, ИСПОЛЬЗУЕМЫХ ДЛЯ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В соответствии с частью 5 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 31.07.2017, N 31, ст. 4736) приказываю:

1. Утвердить прилагаемые:

1.1. Порядок установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической инфраструктуры.

1.2. Технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической инфраструктуры.

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

3. Контроль за исполнением настоящего приказа возложить на заместителя Министра связи и массовых коммуникаций Российской Федерации А.В. Соколова.

Министр
Н.А.НИКИФОРОВ

Утвержден
приказом Министерства связи
и массовых коммуникаций
Российской Федерации
от _____ № ____

Порядок установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической инфраструктуры

1. Настоящий Порядок установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической инфраструктуры (далее – Порядок) определяет единый подход к установке и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры (далее – средства поиска атак, КИИ соответственно).

2. Порядок регулирует взаимодействие федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – Уполномоченный орган ГосСОПКА), федерального органа исполнительной власти по выработке и реализации государственной политики и нормативному правовому регулированию в области связи (далее – Уполномоченный орган в области связи), с операторами связи и субъектами КИИ.

3. Порядок установки и эксплуатации средства поиска атак включает в себя:

определение необходимости и места установки средства поиска атак;

установку средства поиска атак и его подключение к сетям электросвязи;

настройку и проверку работоспособности установленного средства поиска атак;

приемку в эксплуатацию установленного средства поиска атак;

обеспечение непрерывной работы средства поиска атак в круглосуточном режиме;

проведение технического обслуживания, замену и демонтаж установленного средства поиска атак;

обеспечение сохранности установленного средства поиска атак.

4. Необходимость и место установки средства поиска атак на сети электросвязи, обеспечивающие взаимодействие значимых объектов КИИ РФ, определяются Уполномоченным органом ГосСОПКА.

4.1 Информация о необходимости установки средства поиска атак с указанием места установки на сети электросвязи оператора связи, эксплуатационных характеристик устанавливаемого средства поиска атак, организации, которая будет проводить установку и настройку средства поиска атак (далее Организация) и ответственного лица Уполномоченного органа ГосСОПКА направляется в Уполномоченный орган в области связи.

4.2 Уполномоченный орган в области связи в срок не более 7 рабочих дней направляет полученную информацию, предусмотренную пунктом 4.1 настоящего Порядка, в адрес оператора связи.

5. Оператор связи в срок не более 30 рабочих дней с даты получения информации, предусмотренной пунктом 4.1 настоящего Порядка, от Уполномоченного органа в области связи уточняет:

место установки средства поиска атак. В случае технической невозможности установки средства поиска атак на место, определенное Уполномоченным органом ГосСОПКА, оператором связи совместно с ответственным лицом Уполномоченного органа ГосСОПКА и Организации определяется возможное другое место установки;

наличие в месте установки средства поиска атак;

способы подключения средства поиска атак к сетям электросвязи, через которые осуществляется взаимодействие объектов КИИ;

сроки и порядок установки средства поиска атак.

6. Согласованные решения по пункту 5 настоящего Порядка для каждого места установки отражаются на Схеме установки средства поиска атак (далее – Схема установки). Схема установки составляется оператором связи в двух экземплярах (трех экземплярах, в случае привлечения Организации) и согласовывается с Уполномоченным органом ГосСОПКА.

7. Схема установки, подписанная ответственным лицом Уполномоченного органа ГосСОПКА и оператором связи, считается согласованием этой схемы со стороны Уполномоченного органа ГосСОПКА.

8. Установка средства поиска атак и его подключение к сетям электросвязи может проводиться в согласованные с оператором связи сроки ответственными лицами:

Уполномоченного органа ГосСОПКА;

оператора связи или Организации имеющей лицензию на деятельность по технической защите информации;

других организаций, имеющих лицензию на деятельность по технической защите информации.

9. Настройка и проверка работоспособности установленного средства поиска атак проводится лицами, указанными в пункте 8 настоящего Порядка в соответствии с эксплуатационной документацией на данные средства.

10. Прием в эксплуатацию установленного средства поиска атак осуществляется комиссией, назначенной оператором связи, из представителей Уполномоченного органа ГосСОПКА, Организации (иной организации, указанной в пункте 8 настоящего Порядка) и оператора связи.

10.1. По результатам приемки оформляется Акт приемки средства поиска атак (далее – Акт приемки).

В Акте приемки указывается:

наименование объекта связи;

дата приемки средств поиска атак;

фамилия, имя, отчество и должность всех членов комиссии;

место установки средства поиска атак (адрес, помещение);

состав и серийный номер (серийные номера компонентов) установленного средства поиска атак;

результат проверки работоспособности установленного средства поиска атак.

Акт приемки подписывается всеми членами комиссии.

10.2. Схема установки является приложением к Акту приемки.

10.3. Эксплуатация средства поиска атак осуществляется Уполномоченным органом ГосСОПКА.

11. Установка средства поиска атак не требует изменения Схемы организации связи и повторной сдачи объекта связи в эксплуатацию Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.

12. Непрерывность функционирования средства поиска атак в круглосуточном режиме обеспечивается оператором связи путем соблюдения технических условий установки и эксплуатации средства.

13. Техническое обслуживание установленного средства поиска атак проводится ответственными лицами Уполномоченного органа ГосСОПКА или Организацией в соответствии с планом Уполномоченного органа ГосСОПКА.

14. Информацию о сроках и продолжительности проведения технического обслуживания средства поиска атак и лицах, проводящих техническое обслуживание, Уполномоченный орган ГосСОПКА направляет оператору связи не позднее, чем за 7 рабочих дней до начала проведения работ по техническому обслуживанию.

15. Оператор связи обязан обеспечить сохранность установленных средств поиска атак путем ограничения доступа к ним в соответствии с техническими условиями установки и эксплуатации средства поиска атак, требованиями законодательства Российской Федерации.

16. Оператор связи в срок не менее чем за 7 рабочих дней до начала проведения плановых работ, которые могу повлечь нарушение функционирования средства поиска атак, оповещает Уполномоченный орган ГосСОПКА.

Утвержден
приказом Министерства связи
и массовых коммуникаций
Российской Федерации
от _____ № ____

Технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической инфраструктуры

1. Технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической инфраструктуры (далее – Технические условия), определяет общие правила их установки и эксплуатации.

2. Настоящие Технические условия разработаны учетом требований Межгосударственного стандарта ГОСТ 2.114-2016 «Единая система конструкторской документации. Технические условия» и задач, установленных для средств поиска атак в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3. Средство поиска атак должно быть установлено в помещении, в котором обеспечено:

3.1. место, достаточное для установки и эксплуатации средства поиска атак. Оборудование средства поиска атак может устанавливаться на полу, фундаменте, аппаратном столе, полке, конструктиве, а также укрепляться на стене или в стенной нише. В случае размещения оборудования и коммутационных панелей в 19-дюймовом конструктиве предпочтительно планировать установку отдельных 19-дюймовых шкафов и стоек таким образом, чтобы обеспечивался доступ к передней и к задней частям таких шкафов и стоек;

3.2. контроль и ограничение физического доступа персонала к средству поиска атак;

3.3. поддержание температуры и влажности воздуха, в пределах которых может осуществляться нормальная эксплуатация (в соответствии с инструкцией по эксплуатации);

3.4. подключение средства поиска атак к электрической сети;

3.5. подключение к каналу связи, необходимому Федеральному органу исполнительной власти, уполномоченному в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы

Российской Федерации для осуществления эксплуатации средства поиска атак;

3.6. подключение к линиям связи, необходимым для выполнения задач средств поиска атак;

3.7. наличие средств пожарной сигнализации и пожаротушения с возможностью визуального и звукового оповещения.

4. Обеспечение средства поиска атак электропитанием.

4.1. Выделяемая для подключения мощность электрической сети должна превышать не менее чем на 20 процентов мощность, требуемую в соответствии с инструкцией по эксплуатации.

4.2. Электропитание средства поиска атак осуществляется от двух независимых источников. При этом система освещения помещения должно осуществляться от различных панелей силового щитка.

4.3. Средства поиска атак должны обеспечиваться бесперебойным электропитанием.