МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 58753
от "25" июня 2020

ПРИКАЗ

17.03.2020 № 114

Москва

Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации

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, № 31, ст. 4736), Положением о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденным постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418 (Собрание законодательства Российской Федерации 2008, № 23, ст. 2708; 2019, № 36, ст. 5046)

ПРИКАЗЫВАЮ:

1. Утвердить Порядок установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации, согласно приложению 1 к настоящему приказу.

2. Утвердить Технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации, согласно приложению 2 к настоящему приказу.

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

4. Контроль за исполнением настоящего приказа возложить на заместителя Министра цифрового развития, связи и массовых коммуникаций Российской Федерации А.В. Соколова.

Министр М.И. Шадаев

ПРИЛОЖЕНИЕ 1
к приказу Министерства цифрового
развития, связи и массовых
коммуникаций Российской Федерации
от 17.03.2020 г. № 114

ПОРЯДОК

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

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

2. Порядок регулирует процедуру взаимодействия федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[1] (далее – Уполномоченный орган ГосСОПКА), федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативному правовому регулированию в области связи (далее – Уполномоченный орган в области связи) и операторов связи.

3. Установка и эксплуатация средств поиска атак включает в себя:

определение необходимости и мест установки средств поиска атак;

установку средств поиска атак, их подключение к сетям электросвязи и к каналам связи, необходимым для управления средствами поиска атак;

настройку и проверку работоспособности установленных средств поиска атак;

прием в эксплуатацию установленных средств поиска атак;

обеспечение непрерывной работы средств поиска атак;

проведение технического обслуживания, замену и демонтаж установленных средств поиска атак;

обеспечение сохранности установленных средств поиска атак;

---

[1] Указом Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 52, ст.8112) функции федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации возложены на Федеральную службу безопасности Российской Федерации.

осуществление мониторинга за функционированием средств поиска атак.

4. Необходимость и места установки средств поиска атак на сети электросвязи, обеспечивающей взаимодействие объектов КИИ, определяются Уполномоченным органом ГосСОПКА на основании оценки безопасности критической информационной инфраструктуры, проводимой в соответствии с пунктом 4 части 4 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) (далее – Закон).

5. Установку в сетях электросвязи средств поиска атак в соответствии с пунктом 8 части 4 статьи 6 Закона организует Уполномоченный орган ГосСОПКА.

В соответствии с подпунктами 50 и 50.1 пункта 9 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960 (Собрание законодательства Российской Федерации, 2003, № 33, ст. 3254; 2018, № 28, ст. 4198) Уполномоченный орган ГосСОПКА может привлекать организацию для установки средств поиска атак в сетях электросвязи (далее – Организация).

6. Уполномоченный орган ГосСОПКА направляет оператору связи по почте заказным письмом с уведомлением о вручении следующую информацию и документы:

сведения о необходимости установки средств поиска атак с указанием мест установки на сети электросвязи оператора связи;

эксплуатационные характеристики устанавливаемых средств поиска атак;

наименование Организации (в случае привлечения);

фамилия, имя, отчество (при наличии), должность должностного лица Уполномоченного органа ГосСОПКА или наименование структурного подразделения Уполномоченного органа ГосСОПКА, ответственного за организацию работ;

инструкция по эксплуатации средства поиска атак, установка которого планируется на сети электросвязи.

7. Оператор связи не позднее 10 календарных дней с даты получения информации, предусмотренной пунктом 6 настоящего Порядка, определяет должностных лиц оператора связи, допущенных к данной информации.

8. Оператор связи в срок не более 30 календарных дней с даты получения информации, предусмотренной пунктом 6 настоящего Порядка, путем направления в адрес должностного лица (структурного подразделения) Уполномоченного органа ГосСОПКА, ответственного за организацию работ, заказного письма с уведомлением о вручении уточняет следующую информацию:

места установки средств поиска атак;

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

способы подключения средств поиска атак к каналам связи, необходимым Уполномоченному органу ГосСОПКА для управления средствами поиска атак;

сроки и процедура установки средств поиска атак.

В случае технической невозможности установки средств поиска атак на места, определенные Уполномоченным органом ГосСОПКА, оператор связи и Организация по согласованию с Уполномоченным органом ГосСОПКА в порядке, предусмотренном пунктом 6 настоящего Порядка, в срок не более 10 календарных дней со дня установления технической невозможности установки средств поиска атак на места, определенные Уполномоченным органом ГосСОПКА, определяют иные места установки средств поиска атак.

9. Информация по пункту 8 настоящего Порядка для каждого места установки отражаются на Схемах установки средств поиска атак (далее – Схемы установки). Схемы установки составляются оператором связи в двух экземплярах и направляются на согласование в Уполномоченный орган ГосСОПКА в течение 30 рабочих дней с даты получения информации, предусмотренной пунктом 6 настоящего Порядка.

Уполномоченный орган ГосСОПКА обязан в течение 30 календарных дней со дня получения Схем установки принять решение о согласовании Схем установки или об обоснованном отказе в согласовании Схем установки. Указанное решение направляется Уполномоченным органом ГосСОПКА оператору связи не позднее 5 рабочих дней со дня его принятия.

В случае принятия Уполномоченным органом ГосСОПКА решения об обоснованном отказе в согласовании Схем установки оператор связи обязан в течение 15 рабочих дней со дня получения указанного решения внести изменения в Схемы установки и направить Уполномоченному органу ГосСОПКА измененные Схемы установки.

10. Установка средств поиска атак, их подключение к сетям электросвязи и каналам связи проводятся ответственным лицом Уполномоченного органа ГосСОПКА или Организации и оператором связи в срок не более 60 рабочих дней со дня согласования Уполномоченным органом ГосСОПКА Схем установки, если иной срок не согласован Уполномоченным органом ГосСОПКА.

11. При проведении приемки в эксплуатацию средств поиска атак осуществляются настройка и проверка работоспособности установленных средств поиска атак лицами, указанными в пункте 8 настоящего Порядка, в соответствии с эксплуатационной документацией на данные средства.

12. Прием в эксплуатацию установленных средств поиска атак осуществляется комиссией, назначенной оператором связи из представителей Уполномоченного органа ГосСОПКА, Организации (в случае привлечения) и оператора связи.

13. По результатам приемки оформляется Акт приемки средств поиска атак в эксплуатацию (далее – Акт приемки в эксплуатацию).

В Акте приемки в эксплуатацию указываются:

наименование объекта связи;

дата приемки средств поиска атак;

фамилия, имя, отчество (при наличии) и должность каждого члена комиссии;

места установки средств поиска атак (адрес, помещение);

состав и серийные номера (серийные номера компонентов) установленных средств поиска атак;

результат проверки работоспособности установленных средств поиска атак;

схема установки средств поиска атак.

Акт приемки в эксплуатацию подписывается всеми членами комиссии.

14. Эксплуатация средств поиска атак осуществляется Уполномоченным органом ГосСОПКА.

15. Непрерывность функционирования в круглосуточном режиме и сохранность средств поиска атак обеспечиваются оператором связи самостоятельно путем соблюдения утвержденных Уполномоченным органом в области связи технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации (далее – Технические условия).

Для организации взаимодействия с Уполномоченным органом ГосСОПКА оператор связи определяет ответственных лиц.

16. Техническое обслуживание установленных средств поиска атак проводится ответственными лицами Уполномоченного органа ГосСОПКА или Организацией (в случае привлечения).

17. Информацию о сроках и продолжительности проведения технического обслуживания средств поиска атак и лицах, проводящих техническое обслуживание, Уполномоченный орган ГосСОПКА направляет оператору связи по почте заказным письмом с уведомлением о вручении не позднее чем за 7 календарных дней до начала проведения работ по техническому обслуживанию.

18. Оператор связи в срок не менее чем за 14 календарных дней до начала проведения плановых работ, которые могут повлечь нарушение функционирования средств поиска атак, оповещает Уполномоченный орган ГосСОПКА посредством направления уведомления по почте заказным письмом с уведомлением о вручении о сроках и продолжительности проведения указанных плановых работ.

19. Замена средств поиска атак осуществляется в случае нарушения их функционирования или необходимости их модернизации в том же порядке и в те же сроки, что и проведение технического обслуживания средств поиска атак, указанные в пунктах 16 и 17 настоящего Порядка, с оформлением Акта приемки в эксплуатацию, указанного в пункте 13 настоящего Порядка.

20. Демонтаж средств поиска атак проводится в случае необходимости изменения мест установки средств поиска атак или в связи с реорганизацией, ликвидацией или прекращением деятельности оператора связи по решению Уполномоченного органа ГосСОПКА и в срок, согласованный с оператором связи, ответственными лицами Уполномоченного органа ГосСОПКА или Организации.

По результатам демонтажа средств поиска атак Уполномоченным органом ГосСОПКА и оператором связи составляется акт о демонтаже в двух экземплярах, по одному для каждой из сторон.

В Акте демонтажа указываются:

наименование объекта связи;

дата демонтажа средств поиска атак;

фамилия, имя, отчество (при наличии) и должность представителя Уполномоченного органа ГосСОПКА и оператора связи;

места установки средств поиска атак (адрес, помещение), в отношении которых производится демонтаж;

состав и серийные номера (серийные номера компонентов) демонтируемых средств поиска атак.

ПРИЛОЖЕНИЕ 2
к приказу Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации
от 17.03.2020 г. № 114

ТЕХНИЧЕСКИЕ УСЛОВИЯ
установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации

1. Условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации (далее – Технические условия), разработаны с учетом требований к средствам поиска атак в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, установленных приказом Федеральной службы безопасности Российской Федерации от 6 мая 2019 г. № 196 (зарегистрирован Минюстом России 31 мая 2019 г., регистрационный № 54801).

2. Средства поиска атак должны быть установлены в помещениях, в которых обеспечено:

место для установки и непрерывной эксплуатации в круглосуточном режиме средств поиска атак;

контроль и ограничение физического доступа персонала к средствам поиска атак с целью обеспечения их сохранности;

поддержание температуры и влажности воздуха, в пределах которых может осуществляться эксплуатация (в соответствии с инструкцией по эксплуатации средств поиска атак);

выделение маршрутизируемых IP-адресов и подключение средств поиска атак к каналам связи, необходимым федеральному органу исполнительной власти, уполномоченному в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, для управления средствами поиска атак, а также обеспечение функционирования указанных выше каналов связи;

подключение средств поиска атак к линиям связи и средствам связи сетей электросвязи, через которые осуществляется взаимодействие объектов КИИ, необходимым для выполнения задач средств поиска атак;

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

3. Условия обеспечения средств поиска атак электропитанием:

выделяемая для подключения мощность электрической сети должна превышать не менее чем на 20 процентов мощность, требуемую в соответствии с инструкцией по эксплуатации средств поиска атак;

средства поиска атак должны быть подключены к электрическим сетям и обеспечиваться бесперебойным электропитанием.