ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ **Москва** **№**_____

Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими

В соответствии с подпунктом «в» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»[1]

П Р И К А З Ы В А Ю:

утвердить порядок осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими.

Директор А.Бортников

[1] Собрание законодательства Российской Федерации, 2022, № 18, ст. 3058.

Утвержден
приказом ФСБ России
от
№

Порядок
осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими

1. Мониторинг защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими (далее – мониторинг защищенности и органы (организации) соответственно), осуществляется в целях оценки способности информационных ресурсов органов (организаций) противостоять угрозам информационной безопасности и выработки рекомендаций по обеспечению их защищенности.

2. Мониторинг защищенности осуществляется Центром защиты информации и специальной связи Федеральной службы безопасности

Российской Федерации и территориальными органами безопасности (далее – органы безопасности, если не оговорено иное).

3. Мониторинг защищенности осуществляется в отношении следующих информационных ресурсов органов (организаций):

информационных систем (в том числе сайтов в сети «Интернет»);

информационно-телекоммуникационных сетей;

автоматизированных систем управления.

Мониторинг защищенности осуществляется только в отношении информационных ресурсов, имеющих непосредственное подключение к сети «Интернет» и (или) сопряженных с сетью «Интернет» с использованием технологии трансляции сетевых адресов.

4. Для осуществления органами безопасности мониторинга защищенности органы (организации) направляют в Центр защиты информации и специальной связи Федеральной службы безопасности Российской Федерации следующую информацию:

о доменных именах и внешних сетевых адресах принадлежащих (используемых) информационных ресурсов однократно в срок до 1 марта 2023 года;

об изменениях доменных имен и внешних сетевых адресов принадлежащих (используемых) информационных ресурсов, а также о приобретении (начале использования) доменных имен и внешних сетевых адресов новых информационных ресурсов в срок до 7 календарных дней со дня их приобретения (начала использования).

5. Мониторинг защищенности осуществляется непрерывно и включает в себя следующие мероприятия:

сбор и анализ сведений и документов о принадлежащих и используемых органами (организациями) информационных ресурсах;

выявление функционирующих сервисов и обнаружение уязвимостей в информационных ресурсах органов (организаций);

оценка защищенности информационных ресурсов органов (организаций).

6. При осуществлении мониторинга защищенности используются:

сведения и документы о принадлежащих и используемых органами (организациями) информационных ресурсах;

результаты мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в информационных ресурсах органов (организаций), проведенных органами (организациями) и аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА), либо центрами ГосСОПКА, осуществляющими указанные мероприятия на основании заключенных с Федеральной службой безопасности Российской Федерации (Национальным координационным центром по компьютерным инцидентам) соглашений о сотрудничестве (взаимодействии) в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты в течение переходного периода, определенного в соответствии с подпунктом «б» пункта 5 Указа Президента Российской Федерации № 250 от 1 мая 2022 г.[1] (далее – центры ГосСОПКА);

сведения о состоянии защищенности информационных ресурсов органов (организаций), содержащиеся в ГосСОПКА;

сведения, полученные по результатам анализа информации о выявленных сервисах и обнаруженных уязвимостях в информационных ресурсах органов (организаций);

результаты осуществления оценки защищенности информационных ресурсов органов (организаций).

7. В целях проведения мониторинга защищенности органы (организации) и центры ГосСОПКА по запросам органов безопасности

[1] Собрание законодательства Российской Федерации, 2022, № 18, ст. 3058.

представляют в срок до 14 календарных дней со дня получения запроса, сведения, документы и результаты, указанные в абзацах втором и третьем пункта 6 настоящего Порядка.

8. При проведении органами безопасности мероприятий, предусмотренных абзацами третьим и четвертым пункта 5 настоящего Порядка, органы (организации) по запросам органов безопасности обязаны исключить блокировку IP-адресов, с которых осуществляются указанные мероприятия.

9. Запросы, указанные в пунктах 7 и 8 настоящего Порядка, могут быть направлены в органы (организации) по почте заказным письмом, в электронном виде по адресам электронной почты, а также могут быть вручены под роспись должностному лицу органа (организации).

10. Выявление функционирующих сервисов и обнаружение уязвимостей в информационных ресурсах органов (организаций) осуществляются удаленно без предварительного уведомления органов (организаций) о начале проведения указанных мероприятий.

11. Оценка защищенности информационных ресурсов органов (организаций) осуществляется органами безопасности на основании ежегодного плана, утверждаемого начальником Центра защиты информации и специальной связи Федеральной службы безопасности Российской Федерации, формируемого, в том числе на основании предложений территориальных органов безопасности.

Выписки из указанного плана направляются территориальным органам безопасности, а также органам (организациям), в отношении информационных ресурсов которых предусмотрено проведение оценки защищенности.

12. О проведении оценки защищенности информационных ресурсов органы (организации) письменно уведомляются органами безопасности не позднее чем за 14 календарных дней до начала проведения указанных мероприятий.

13. Для оценки защищенности информационных ресурсов органов (организаций) осуществляется подключение программно-аппаратных комплексов органов безопасности к информационным ресурсам органов (организаций). Подключение программно-аппаратных комплексов органов безопасности к информационным ресурсам органов (организаций) может осуществляться как удаленно, так и на объектах органов (организаций).

14. При выявлении в ходе оценки защищенности информационных ресурсов органов (организаций) признаков нарушения штатного режима их функционирования орган (организация) незамедлительно информирует об этом орган безопасности.

При поступлении от органа (организации) указанной информации проведение оценки защищенности информационных ресурсов органа (организации) приостанавливается до выяснения и ликвидации причин возникновения нарушения штатного режима их функционирования.

15. В случае выявления в рамках осуществления мониторинга защищенности неспособности информационных ресурсов противостоять угрозам информационной безопасности, органом безопасности выдается указание[1] по обеспечению защищенности принадлежащих и используемых органом (организации) информационных ресурсов.

16. На основании результатов, полученных органом безопасности в рамках мониторинга защищенности, Центром защиты информации и специальной связи Федеральной службы безопасности Российской Федерации подготавливаются и направляются в органы (организации) рекомендации по обеспечению защищенности информационных ресурсов.

---

[1] Подпункт «д» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».