Приказ Федеральной службы безопасности Российской Федерации от 11.05.2023 г. № 213
(Официальный интернет-портал правовой информации (www.pravo.gov.ru) от 02.06.2023 г., ст. 0001202306020020)

Исходная редакция

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

Москва

11 мая 2023 г. № 213

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

Зарегистрирован Минюстом России 2 июня 2023 г.
Регистрационный № 73701

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"

ПРИКАЗЫВАЮ:

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

Утвержден
приказом ФСБ России
от 11 мая 2023 г. № 213

Порядок осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям) и 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) и 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.

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 только в отношении информационных ресурсов, имеющих непосредственное подключение к информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") и (или) сопряженных с сетью "Интернет" с использованием технологии трансляции сетевых адресов.

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.

При осуществлении мониторинга защищенности руководители органов (организаций) обязаны обеспечивать должностным лицам органов безопасности беспрепятственный доступ[1] (в том числе удаленный) к принадлежащим органам (организациям) либо используемым ими информационным ресурсам.

---

[1] Подпункт "д" пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250.

4. Для осуществления органами безопасности мониторинга защищенности органы (организации) должны направить на адрес электронной почты monitoring@fsb.ru следующую информацию:

о доменных именах и внешних сетевых адресах информационных ресурсов, принадлежащих органам (организациям) либо используемых ими, а также об адресах электронной почты, предназначенных для ведения переписки с органами безопасности по вопросам осуществления мониторинга защищенности, - однократно в срок до 1 сентября 2023 г.;

об изменениях доменных имен, внешних сетевых адресов информационных ресурсов, принадлежащих органам (организациям) либо используемых ими, а также о приобретении (начале использования) доменных имен и внешних сетевых адресов новых информационных ресурсов - в срок до 7 рабочих дней со дня их приобретения (начала использования);

об изменении (начале использования) адреса электронной почты, предназначенного для ведения переписки с органами безопасности по вопросам осуществления мониторинга защищенности, - в срок до 7 рабочих дней со дня его изменения (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 от 1 мая 2022 г. № 250 (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 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. Документы, подготавливаемые органами безопасности в соответствии с настоящим Порядком, могут быть направлены в органы (организации) по почте заказным письмом, в электронном виде по адресам электронной почты, а также могут быть вручены под подпись должностному лицу органа (организации).

Документы, подготавливаемые органами (организациями) в соответствии с настоящим Порядком, могут быть направлены в Центр защиты информации и специальной связи Федеральной службы безопасности Российской Федерации по почте заказным письмом или в электронном виде на адрес электронной почты, указанный в пункте 4 настоящего Порядка, а также могут быть вручены под подпись должностному лицу Центра защиты информации и специальной связи Федеральной службы безопасности Российской Федерации.

Документы, подготавливаемые органами (организациями) в соответствии с настоящим Порядком, могут быть направлены в территориальный орган безопасности по

почте заказным письмом или в электронном виде на адрес электронной почты соответствующего территориального органа безопасности, указанный на официальном сайте Федеральной службы безопасности Российской Федерации в сети "Интернет" по адресу: www.fsb.ru, а также могут быть вручены под подпись должностному лицу территориального органа безопасности.

Документы, направляемые органами (организациями), подписываются руководителем органа (организации) или заместителем руководителя органа (организации), на которого возложены полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты.

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 заместителем руководителя Научно-технической службы - 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.

В уведомлении указываются орган безопасности, проводящий оценку защищенности, даты начала и окончания ее проведения, контактный телефон органа безопасности.

13. Оценка защищенности информационных ресурсов органов (организаций) осуществляется в том числе с использованием подключаемых к информационным ресурсам органов (организаций), указанным в пункте 3 настоящего Порядка, программно-аппаратных комплексов органов безопасности. 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, приводящего к невозможности реализации информационными ресурсами основного функционала, орган (организация) не позднее двух часов с момента выявления таких признаков письменно уведомляет об этом орган безопасности.

В течение двух часов с момента поступления указанной информации проведение оценки защищенности информационных ресурсов органа (организации)

приостанавливается для выяснения и ликвидации органом (организацией) причин возникновения нарушения штатного режима их функционирования.

Проведение оценки защищенности информационных ресурсов органов (организаций) возобновляется через шесть часов с момента ее приостановления.

В случае невозможности восстановления органами (организациями) штатного режима функционирования информационных ресурсов в течение шести часов с момента приостановления проведения оценки защищенности в орган безопасности направляется обоснование невозможности возобновления ее проведения с указанием срока устранения причин приостановления.

По результатам рассмотрения указанного обоснования орган безопасности в течение двадцати четырех часов с момента его получения принимает решение о продолжении либо о прекращении проведения оценки защищенности до устранения причин ее приостановления.

О принятом решении орган безопасности в течение двух часов с момента его принятия письменно информирует орган (организацию).

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 органу (организации) либо используемых ими информационных ресурсов.

---

[1] Подпункт "д" пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250.