

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ
О ДОПОЛНИТЕЛЬНЫХ МЕРАХ
ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

В целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации постановляю:

1. Руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее - органы (организации)):

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;

в) принимать в случае необходимости решения о привлечении организаций к осуществлению мероприятий по обеспечению информационной безопасности органа (организации). При этом могут привлекаться исключительно организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации;

г) принимать в случае необходимости решения о привлечении организаций к осуществлению мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. При этом могут привлекаться исключительно организации, являющиеся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, за исключением случая, предусмотренного подпунктом "б" пункта 5 настоящего Указа;

д) обеспечивать должностным лицам органов федеральной службы безопасности беспрепятственный доступ (в том числе удаленный) к принадлежащим органам (организациям) либо используемым ими информационным ресурсам, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет", в целях осуществления мониторинга, предусмотренного подпунктом "в" пункта 5 настоящего Указа, а также обеспечивать исполнение указаний, данных органами федеральной службы безопасности по результатам такого мониторинга;

е) обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их компетенции и направляются на регулярной основе в органы (организации) с учетом меняющихся угроз в информационной сфере.

2. Возложить на руководителей органов (организаций) персональную ответственность за обеспечение информационной безопасности соответствующих органов (организаций).

3. Правительству Российской Федерации в месячный срок:

а) утвердить:

типовое положение о заместителе руководителя органа (организации), ответственного за

обеспечение информационной безопасности органа (организации);

типовое положение о структурном подразделении органа (организации), обеспечивающем информационную безопасность органа (организации);

б) определить перечень ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

4. Органам (организациям), включенным в перечень, определенный в соответствии с подпунктом "б" пункта 3 настоящего Указа, осуществить мероприятия по оценке уровня защищенности своих информационных систем и до 1 июля 2022 г. представить доклад в Правительство Российской Федерации.

5. Федеральной службе безопасности Российской Федерации:

а) организовать аккредитацию центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

б) определить переходный период, в течение которого допускается осуществлять мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в интересах органов (организаций) 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) определить порядок осуществления мониторинга защищенности информационных ресурсов, принадлежащих органам (организациям) либо используемых ими, и осуществлять такой мониторинг.

6. Установить, что с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

7. Настоящий Указ вступает в силу со дня его официального опубликования.

Президент
Российской Федерации
В.ПУТИН

Москва, Кремль

1 мая 2022 года

N 250
