

Статья 6. Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры

1. Президент Российской Федерации определяет:

- 1) основные направления государственной политики в области обеспечения безопасности критической информационной инфраструктуры;
- 2) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
- 3) федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
- 4) порядок создания и задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

2. Правительство Российской Федерации устанавливает:

- 1) показатели критериев значимости объектов критической информационной инфраструктуры и их значения, а также порядок и сроки осуществления их категорирования;
- 2) порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;
- 3) порядок подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры.

3. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации:

- 1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Президенту Российской Федерации и (или) в Правительство Российской Федерации;
- 2) утверждает порядок ведения реестра значимых объектов критической информационной инфраструктуры и ведет данный реестр;
- 3) утверждает форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;
- 4) устанавливает требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры (требования по обеспечению безопасности информационно-телекоммуникационных сетей, которым присвоена одна из категорий значимости и которые включены в реестр значимых объектов критической информационной инфраструктуры, устанавливаются по согласованию с федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи), а также требования к созданию систем безопасности таких объектов и обеспечению их функционирования (в банковской сфере и в иных сферах финансового рынка устанавливает указанные требования по согласованию с Центральным банком Российской Федерации);
- 5) осуществляет государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также утверждает форму акта проверки, составляемого по итогам проведения указанного контроля.

4. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:
- 1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Президенту Российской Федерации и (или) в Правительство Российской Федерации;
 - 2) создает национальный координационный центр по компьютерным инцидентам и утверждает положение о нем;
 - 3) координирует деятельность субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
 - 4) организует и проводит оценку безопасности критической информационной инфраструктуры;
 - 5) определяет перечень информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и порядок ее представления;
 - 6) утверждает порядок информирования федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры (в банковской сфере и в иных сферах финансового рынка утверждает указанный порядок по согласованию с Центральным банком Российской Федерации);
 - 7) утверждает порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, а также порядок получения субъектами критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения;
 - 8) организует установку на значимых объектах критической информационной инфраструктуры и в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
 - 9) устанавливает требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
 - 10) утверждает порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры (в банковской сфере и в иных сферах финансового рынка утверждает указанные порядок и технические условия по согласованию с Центральным банком Российской Федерации).
5. Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи, утверждает по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и

ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, порядок, технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры.