Постановление Правительства РФ от 17.02.2018 № 162 "Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"

В соответствии с пунктом 2 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» Правительство Российской Федерации постановляет:

Утвердить прилагаемые Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Председатель Правительства
Российской Федерации
Д.Медведев

Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Утверждены
постановлением Правительства
Российской Федерации
от 17 февраля 2018 г. № 162

I. Общие положения

1. Настоящие Правила устанавливают порядок осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, и его территориальными органами (далее - орган государственного контроля) мероприятий по государственному контролю в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее соответственно - критическая информационная инфраструктура, государственный контроль).

2. Государственный контроль проводится в целях проверки соблюдения субъектами критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, требований, установленных Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» и принятыми в соответствии с ним нормативными правовыми актами (далее соответственно - требования по обеспечению безопасности, проверка).

3. Государственный контроль осуществляется путем проведения плановых и внеплановых выездных проверок.

4. Для осуществления проверки органом государственного контроля создается комиссия в составе не менее 2 должностных лиц. Внеплановая проверка, проводимая по основанию, указанному в подпункте «а» пункта 20 настоящих Правил, может осуществляться одним должностным лицом органа государственного контроля.

5. Проверка проводится должностными лицами органа государственного контроля, которые указаны в приказе органа государственного контроля о проведении проверки.

6. Срок проведения плановой проверки не должен превышать 20 рабочих дней.

7. Срок проведения внеплановой проверки не должен превышать 10 рабочих дней.

8. Срок проведения каждой из проверок, предусмотренных пунктом 3 настоящих Правил, в отношении субъекта критической информационной инфраструктуры, который осуществляет свою деятельность на территориях нескольких субъектов Российской Федерации, устанавливается отдельно по каждому филиалу, представительству и обособленному структурному подразделению субъекта критической информационной инфраструктуры, при этом общий срок проведения проверки не может превышать 60 рабочих дней.

9. Проверки в отношении значимых объектов критической информационной инфраструктуры, которые на праве собственности, аренды или ином законном основании принадлежат Министерству обороны Российской Федерации, Службе внешней разведки Российской Федерации, Федеральной службе безопасности Российской Федерации, Федеральной службе охраны Российской Федерации и Главному управлению специальных программ Президента Российской Федерации, а также значимых объектов критической информационной инфраструктуры, защита которых входит в их компетенцию, проводятся по согласованию с

руководителями указанных федеральных органов исполнительной власти.

10. Информация об организации проверок, в том числе об их планировании, о проведении и результатах таких проверок, в органы прокуратуры не направляется, за исключением информации о результатах проверок, проведенных на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

II. Организация плановой проверки

11. Предметом плановой проверки является соблюдение субъектом критической информационной инфраструктуры требований по обеспечению безопасности.

12. Основаниями для осуществления плановой проверки являются истечение 3 лет со дня:
а) внесения сведений об объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры;
б) окончания осуществления последней плановой проверки в отношении значимого объекта критической информационной инфраструктуры.

13. Ежегодный план проведения плановых проверок утверждается руководителем органа государственного контроля до 20 декабря года, предшествующего году проведения плановых проверок.

14. Ежегодный план проведения плановых проверок содержит следующую информацию:
а) сведения о субъекте критической информационной инфраструктуры;
б) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;
в) дату окончания последней плановой проверки;
г) месяц и срок проведения проверки;
д) основание проведения проверки;
е) наименование органа государственного контроля.

15. Выписки из утвержденного ежегодного плана проведения плановых проверок направляются до 1 января года проведения плановых проверок органом государственного контроля субъектам критической информационной инфраструктуры.

16. О проведении плановой проверки субъект критической информационной инфраструктуры уведомляется органом государственного контроля не менее чем за 3 рабочих дня до начала ее проведения посредством направления копии приказа органа государственного контроля о проведении плановой проверки любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления.

17. Плановая проверка проводится на основании утвержденного ежегодного плана проведения плановых проверок и приказа органа государственного контроля о проведении проверки.

18. В приказе органа государственного контроля о проведении проверки указываются:
а) наименование органа государственного контроля, номер и дата издания приказа;
б) должности, фамилии, имена и отчества должностных лиц органа государственного контроля, уполномоченных на проведение проверки;
в) сведения о субъекте критической информационной инфраструктуры;
г) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;
д) задачи проверки;
е) дата начала и окончания проверки;
ж) срок проведения проверки;
з) правовые основания проведения проверки, в том числе нормативные правовые акты, соблюдение положений которых подлежит проверке;
и) перечень мероприятий по контролю, необходимых для выполнения задач проверки.

III. Организация внеплановой проверки

19. Предметом внеплановой проверки является соблюдение субъектом критической информационной инфраструктуры требований по обеспечению безопасности, выполнение предписания органа государственного контроля, а также проведение мероприятий по предотвращению негативных последствий на значимом объекте критической информационной инфраструктуры, причиной которых является возникновение компьютерного инцидента.

20. Основаниями для осуществления внеплановой проверки являются:
а) истечение срока выполнения субъектом критической информационной инфраструктуры выданного органом государственного контроля предписания об устранении выявленного нарушения требований по обеспечению безопасности;
б) возникновение компьютерного инцидента на значимом объекте критической информационной инфраструктуры, повлекшего негативные последствия;
в) приказ органа государственного контроля, изданный в соответствии с поручением Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора об осуществлении внеплановой проверки в

рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

21. О проведении внеплановой проверки (за исключением внеплановой проверки, основание для осуществления которой указано в подпункте «б» пункта 20 настоящих Правил) субъект критической информационной инфраструктуры уведомляется органом государственного контроля не менее чем за 24 часа до начала ее проведения любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления.

22. В случае если внеплановая проверка проводится по основанию, указанному в подпункте «б» пункта 20 настоящих Правил, орган государственного контроля вправе приступить к проведению внеплановой проверки незамедлительно.

23. Внеплановая проверка проводится на основании приказа органа государственного контроля о проведении проверки, оформленного в соответствии с пунктом 18 настоящих Правил.

IV. Проведение проверки

24. Плановая и внеплановая проверка проводится по месту нахождения субъекта критической информационной инфраструктуры, лица, эксплуатирующего значимый объект критической информационной инфраструктуры, и значимого объекта критической информационной инфраструктуры.

25. Проверка начинается с предъявления служебного удостоверения должностными лицами органа государственного контроля, обязательного ознакомления руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица с приказом органа государственного контроля о проведении проверки.

26. Руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу под расписку передается копия приказа органа государственного контроля о проведении проверки, заверенная печатью органа государственного контроля.

27. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо обязаны предоставить должностным лицам органа государственного контроля, осуществляющим проверку, возможность ознакомиться с документами, связанными с предметом и задачами проверки, а также обеспечить с учетом требований пропускного режима беспрепятственный доступ проводящих проверку должностных лиц на территорию, в используемые при осуществлении деятельности здания, строения, сооружения, помещения и к значимым объектам критической информационной инфраструктуры.

28. Для оценки эффективности принимаемых мер во исполнение требований по обеспечению безопасности должностными лицами органа государственного контроля используются сертифицированные по требованиям безопасности информации программные и аппаратно-программные средства контроля, в том числе имеющиеся у субъекта критической информационной инфраструктуры.

Возможность и порядок использования таких средств контроля с учетом особенностей функционирования значимого объекта критической информационной инфраструктуры согласовывается с руководителем субъекта критической информационной инфраструктуры или уполномоченным им должностным лицом.

V. Ограничения при проведении проверки

29. При проведении проверки должностные лица органа государственного контроля не вправе:
а) проверять выполнение требований по обеспечению безопасности, если они не относятся к полномочиям органа государственного контроля, от имени которого действуют эти должностные лица;
б) проводить проверку в случае отсутствия при ее проведении руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица, за исключением случая проведения проверки по основанию, указанному в подпункте «б» пункта 20 настоящих Правил;
в) требовать представления документов и информации, если они не относятся к предмету проверки, а также изымать оригиналы таких документов;
г) распространять информацию, полученную в результате проведения проверки и составляющую государственную, коммерческую, служебную и иную охраняемую законом тайну, за исключением случаев, предусмотренных законодательством Российской Федерации;
д) превышать установленные сроки проведения проверки;
е) осуществлять выдачу субъектам критической информационной инфраструктуры предписаний или предложений о проведении за их счет мероприятий по контролю;
ж) осуществлять действия с техническими средствами обработки информации, в результате которых может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры.

VI. Обязанности должностных лиц органа государственного контроля при проведении проверки

30. Должностные лица органа государственного контроля при проведении проверки обязаны:

а) своевременно и в полной мере исполнять предоставленные в соответствии с законодательством Российской Федерации полномочия по предупреждению, выявлению и пресечению нарушений субъектом критической информационной инфраструктуры требований по обеспечению безопасности;
б) соблюдать права и законные интересы субъекта критической информационной инфраструктуры, проверка которого проводится;
в) проводить проверку на основании приказа органа государственного контроля о ее проведении в соответствии с ее предметом и задачами;
г) проводить проверку во время исполнения служебных обязанностей и при предъявлении служебных удостоверений и копии приказа органа государственного контроля о проведении проверки;
д) не препятствовать руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу присутствовать при проведении проверки и давать разъяснения по вопросам, относящимся к предмету проверки;
е) предоставлять руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу, присутствующим при проведении проверки, информацию и документы, относящиеся к предмету проверки;
ж) знакомить руководителя субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо с результатами проверки;
з) соблюдать сроки проведения проверки, установленные настоящими Правилами;
и) не требовать от субъекта критической информационной инфраструктуры документы и иные сведения, представление которых не предусмотрено законодательством Российской Федерации;
к) в случае, предусмотренном внутренним распорядком субъекта критической информационной инфраструктуры, пройти в первый день проверки инструктаж по соблюдению техники безопасности при нахождении на территории, на которой расположен проверяемый значимый объект критической информационной инфраструктуры;
л) осуществлять запись о проведенной проверке в журнале учета проверок при его наличии.

VII. Порядок оформления результатов проверки

31. По результатам проверки должностными лицами органа государственного контроля, проводящими проверку, составляется акт проверки.

32. Форма акта проверки утверждается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

33. В акте проверки указываются:
а) дата и место составления акта проверки;
б) наименование органа государственного контроля;
в) дата и номер приказа органа государственного контроля о проведении проверки;
г) продолжительность и место проведения проверки;
д) фамилии, имена, отчества и должности лиц, проводивших проверку;
е) сведения о субъекте критической информационной инфраструктуры;
ж) фамилия, имя и отчество руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица, присутствовавших при проведении проверки;
з) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;
и) сведения о проверяемом значимом объекте критической информационной инфраструктуры;
к) сведения о результатах проверки, в том числе о выявленных нарушениях требований по обеспечению безопасности;
л) сведения о внесении в журнал учета проверок записи о проведенной проверке либо о невозможности внесения такой записи в связи с отсутствием у субъекта критической информационной инфраструктуры указанного журнала;
м) подписи должностных лиц органа государственного контроля, проводивших проверку;
н) сведения об ознакомлении или отказе от ознакомления с актом проверки руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица.

34. На основании акта проверки в случае выявления нарушения требований по обеспечению безопасности орган государственного контроля выдает субъекту критической информационной инфраструктуры предписание об устранении выявленного нарушения с указанием срока его устранения.

35. К акту проверки прилагаются протоколы или заключения по результатам контрольных мероприятий, проведенных с использованием программных и аппаратно-программных средств контроля, а также предписания об устранении выявленных нарушений и иные связанные с результатами проверки документы или их копии.

36. Акт проверки оформляется непосредственно после ее завершения в 3 экземплярах, один из которых с приложениями вручается руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу. Второй экземпляр акта проверки направляется в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, третий - в территориальный орган федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры, проводивший проверку.

37. В случае проведения внеплановой проверки на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям копия акта проверки с копиями приложений высылается в соответствующий орган прокуратуры.

38. Результаты проверки, содержащие информацию, составляющую государственную, коммерческую, служебную и иную

охраняемую законом тайну, оформляются с соблюдением требований, предусмотренных законодательством Российской Федерации.

VIII. Меры, принимаемые должностными лицами органа государственного контроля в отношении фактов нарушения требований по обеспечению безопасности, выявленных при проведении проверки

39. В случае выявления при проведении проверки нарушения субъектом критической информационной инфраструктуры требований по обеспечению безопасности должностные лица органа государственного контроля, проводившие проверку, в пределах полномочий, предусмотренных законодательством Российской Федерации, обязаны:
а) выдать предписание субъекту критической информационной инфраструктуры об устранении выявленного нарушения требований по обеспечению безопасности с указанием срока его устранения, который устанавливается в том числе с учетом утвержденных и представленных субъектом критической информационной инфраструктуры программ (планов) по модернизации (дооснащению) значимого объекта критической информационной инфраструктуры;
б) принять меры по контролю за устранением выявленного нарушения, его предупреждению и предотвращению.

40. В случае невозможности выполнения предписания, предусмотренного подпунктом «а» пункта 39 настоящих Правил, по причинам, не зависящим от субъекта критической информационной инфраструктуры, руководитель органа государственного контроля при поступлении в орган государственного контроля мотивированного обращения субъекта критической информационной инфраструктуры вправе продлить срок выполнения указанного предписания, но не более чем на один год, уведомив об этом субъекта критической информационной инфраструктуры в течение 30 дней со дня регистрации указанного обращения.

IX. Ответственность органа государственного контроля и его должностных лиц при проведении проверки

41. Орган государственного контроля и его должностные лица в случае ненадлежащего исполнения соответственно функций, служебных обязанностей и совершения противоправных действий (бездействия) при проведении проверки несут ответственность в соответствии с законодательством Российской Федерации.

42. Орган государственного контроля осуществляет контроль за исполнением должностными лицами органа государственного контроля служебных обязанностей, ведет учет случаев ненадлежащего исполнения должностными лицами служебных обязанностей, проводит соответствующие служебные проверки и принимает в соответствии с законодательством Российской Федерации меры в отношении таких должностных лиц.

43. Орган государственного контроля обязан сообщить в письменной форме субъекту критической информационной инфраструктуры, права и (или) законные интересы которого нарушены, о мерах, принятых в отношении виновных в нарушении законодательства Российской Федерации должностных лиц, в течение 10 дней со дня принятия таких мер.

X. Недействительность результатов проверки, проведенной с грубым нарушением положений настоящих Правил

44. Результаты проверки, проведенной органом государственного контроля с грубым нарушением положений настоящих Правил, не могут являться доказательствами нарушения субъектом критической информационной инфраструктуры требований по обеспечению безопасности и подлежат отмене органом государственного контроля на основании заявления субъекта критической информационной инфраструктуры.

45. К грубым нарушениям положений настоящих Правил относятся:
а) отсутствие оснований для проведения проверки;
б) нарушение срока уведомления о проведении проверки;
в) нарушение срока проведения проверки;
г) проведение проверки без приказа органа государственного контроля;
д) невручение руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу акта проверки;
е) проведение плановой проверки, не включенной в ежегодный план проведения плановых проверок.

XI. Права, обязанности и ответственность субъекта критической информационной инфраструктуры при осуществлении государственного контроля

46. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо при проведении проверки имеют право:
а) получать от органа государственного контроля и его должностных лиц информацию, которая относится к предмету проверки и представление которой предусмотрено настоящими Правилами;
б) знакомиться с результатами проверки и указывать в акте проверки о своем ознакомлении с результатами проверки, согласии или несогласии с ними, а также с отдельными действиями должностных лиц органа государственного контроля;
в) обжаловать действия (бездействие) должностных лиц органа государственного контроля, повлекшие за собой нарушение прав субъекта критической информационной инфраструктуры при проведении проверки, в административном и (или) судебном порядке в соответствии с законодательством Российской Федерации.

47. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо при проведении проверки обязаны:
а) непосредственно присутствовать при проведении проверки и давать пояснения по вопросам, относящимся к предмету проверки;
б) предоставить должностным лицам органа государственного контроля, проводящим проверку, возможность ознакомиться с документами, связанными с задачами и предметом проверки;
в) выполнять предписания должностных лиц органа государственного контроля об устранении нарушений в части соблюдения требований по обеспечению безопасности, выданные этими лицами в соответствии со своей компетенцией;
г) обеспечить с учетом требований пропускного режима беспрепятственный доступ проводящих проверку должностных лиц на территорию, в используемые при осуществлении деятельности здания, строения, сооружения, помещения и к значимым объектам критической информационной инфраструктуры;
д) в случае, предусмотренном внутренним распорядком субъекта критической информационной инфраструктуры, провести в первый день проверки инструктаж по соблюдению техники безопасности при нахождении на территории, на которой расположен проверяемый значимый объект критической информационной инфраструктуры, с должностными лицами органа государственного контроля, осуществляющими проверку;
е) принимать меры по устранению выявленных нарушений.

48. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо, допустившие нарушение положений настоящих Правил, необоснованно препятствующие проведению проверки, уклоняющиеся от проведения проверки и (или) не выполняющие в установленный срок предписания органа государственного контроля об устранении выявленных нарушений требований по обеспечению безопасности, несут ответственность в соответствии с законодательством Российской Федерации.

49. В случае невозможности выполнения предписания, предусмотренного подпунктом «а» пункта 39 настоящих Правил, по причинам, не зависящим от субъекта критической информационной инфраструктуры, субъект критической информационной инфраструктуры до истечения срока выполнения предписания вправе обратиться с мотивированным обращением о продлении срока выполнения предписания к руководителю органа государственного контроля, выдавшему такое предписание. Обращение субъекта критической информационной инфраструктуры подлежит рассмотрению в порядке, предусмотренном пунктом 40 настоящих Правил.

50. В случае несогласия с фактами, изложенными в акте проверки и (или) предписании об устранении выявленного нарушения, руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо вправе представить в течение 15 дней с даты получения акта проверки в проводивший проверку орган государственного контроля возражения в письменной форме в отношении акта проверки и (или) выданного предписания об устранении выявленного нарушения в целом или их отдельных положений. При этом субъект критической информационной инфраструктуры вправе приложить к возражениям документы, подтверждающие обоснованность таких возражений, или их заверенные копии либо в согласованный срок передать их в орган государственного контроля.

безопасность критической информационной инфраструктуры, государственная тайна, коммерческая тайна, служебная тайна, фстэк

From:
http://www.sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://www.sps-ib.ru/npa:pp162_17.02.2018

Last update: **2018/02/25 18:35**